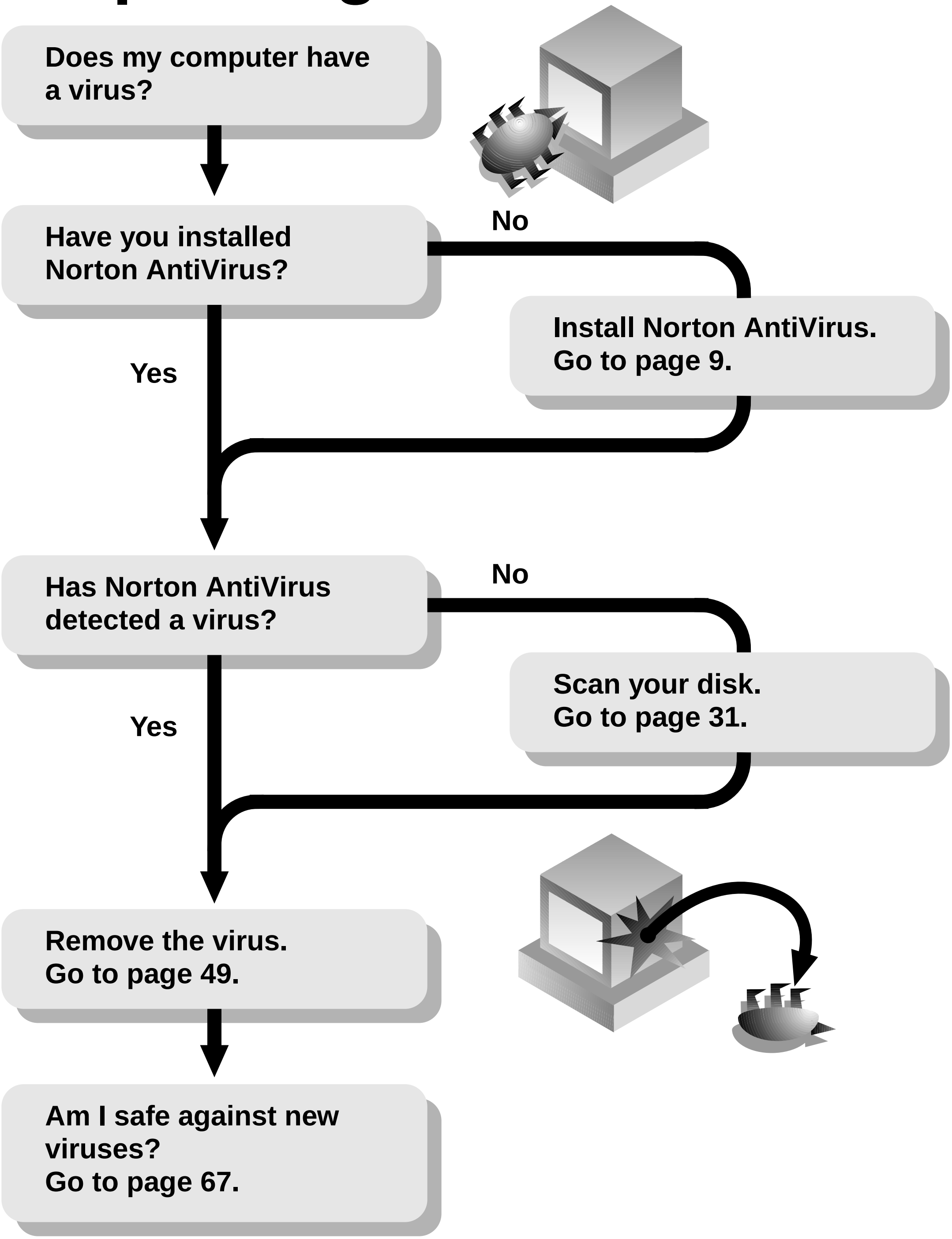
Reference Guide

SYMANTEC.™

NORTON AntiVirus™

Version 4.0

Help! I’ve got a virus!



Does my computer have a virus?

Have you installed Norton AntiVirus?

No

Install Norton AntiVirus. Go to page 9.

Yes

Has Norton AntiVirus detected a virus?

No

Scan your disk. Go to page 31.

Yes

Remove the virus. Go to page 49.

Am I safe against new viruses? Go to page 67.

Norton AntiVirus™ for Windows® 95 Reference Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec, Norton AntiVirus, Symantec AntiVirus for Macintosh, and Norton Utilities are trademarks of Symantec Corporation.

Windows is a registered trademark and Windows 95 is a trademark of Microsoft Corporation. NetWare is a trademark of Novell Corporation. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

• You may:
(i) use only one copy of one version of the various versions of the Software contained on the enclosed CD-ROM on a single computer;

(ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;

(iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;

(iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and

(v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

• You may not:
(i) copy the documentation which accompanies the Software;
(ii) sublicense, rent or lease any portion of the Software;
(iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
(iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

• Sixty Day Money Back Guarantee:
If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

• Limited Warranty:
Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.
THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

• Disclaimer of Damages:
REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

• U.S. Government Restricted Rights:
RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

• General:
This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 10201 Torre Avenue, Cupertino, CA 95014.

Contents

Installation

Quickstart

Chapter 1 About Norton AntiVirus

Chapter 2 Using Norton AntiVirus

Chapter 3 Eliminating viruses

Chapter 4 Keeping up with new viruses

Chapter 5 Customizing Norton AntiVirus

Appendix A About computer viruses

Appendix B Using your Norton AntiVirus rescue disks

Appendix C Using command-line switches

Appendix D System messages

Appendix E Troubleshooting

Glossary

Symantec Service and Support Solutions

Disk Exchange and/or Replacement Form

Potential Virus Submission Procedure

Index

Installation

When you install Norton AntiVirus exactly as directed by the on-screen messages, you will have complete virus protection as soon as you restart your computer. This includes:

- Norton AntiVirus loaded automatically each time you start your computer
- Rescue Disks to protect you in case you can't start your computer
- An automatic scan of your disks once per week to ensure they stay virus-free.
- Protection when you download files from the Internet

Requirements for installing

Your minimum computer requirements are:

- 486 IBM or compatible PC with 8 MB of memory
- Microsoft Windows 95
- 10 MB of free hard disk space to install Norton AntiVirus

You also must have:

- Three 1.44 MB floppy disks and three disk labels (for Rescue Disks)

WHY? The last step of Install asks you to create Rescue Disks. These Rescue Disks are an important part of your virus protection. For example, they allow you to safely restart your computer if it is halted due to a virus in memory.

Installing Norton AntiVirus for Windows 95

For the most complete protection, simply click Next on all the setup panels to accept the preset options.

To start install:

1. Do one of the following:
   - For a CD-ROM, insert the CD into the CD-ROM drive. The Norton AntiVirus setup program starts automatically.

- For floppy disks, insert Norton AntiVirus Disk 1 in the A: drive, click Start on the Windows taskbar, click Run, type `A:SETUP` in the text box, then click OK.

2 Follow the on-screen instructions. Questions? See page 10.

If Norton AntiVirus can't install because it finds a virus, see "Removing viruses when you install" in this section.

3 Test your Norton AntiVirus Emergency Boot Disk. See page 12 for testing details.

Removing viruses when you install

When you install Norton AntiVirus, it scans for viruses. If it finds an active virus, you will have to use the Emergency Boot disk that comes with the product to remove the virus before you can finish installing.

To remove the virus:

1 Turn off your computer using the power switch.

2 Insert the Emergency Boot Disk that came with Norton AntiVirus in your A: drive.

3 Turn on your computer.

The Norton AntiVirus Emergency Disk dialog box appears.

4 Press Enter to start the Emergency program.

The Emergency program takes several minutes to load, then automatically scans your computer and removes viruses.

Questions when installing

Norton AntiVirus helps you install by giving you on-screen directions and highlighting the recommended actions. You are asked to make the following choices:

What the choices are	What you should do	Why?
Select the folder for Norton AntiVirus.	Accept the preset choice: C:\Program Files\Norton AntiVirus	There's no reason not to. The choice is there for unusual circumstances.
Schedule weekly scans of your local hard disks that run automatically.	Leave this checked.	A weekly scan makes sure your disks stay virus-free.
Automatically start Auto-Protect.	Leave this checked.	Auto-Protect constantly monitors your computer to make sure a virus does not gain entry.
Scan at startup.	Leave this checked.	Makes sure critical system files are virus-free every time you start up.
Norton AntiVirus has detected a Netscape browser. Do you want to install plug-ins?	Choose Yes.	This option allows Norton AntiVirus to scan files for viruses when you download using a Netscape browser.
Do you wish to create Rescue Disks?	We highly recommend that you create the Rescue Disks.	Rescue Disks can save you from disaster if your computer becomes infected with certain types of viruses.
Run LiveUpdate after installation.	Leave this checked if you have a modem or Internet connection.	LiveUpdate connects to a special Symantec site and updates Norton AntiVirus automatically to protect you against newly discovered viruses.
Scan for viruses after installation.	Leave this checked.	Makes sure that your computer is virus-free.
Would you like to restart your computer?	Select Yes, I want to restart my computer now.	When your computer restarts, you are fully protected against viruses.

Testing the Norton AntiVirus Emergency Boot Disk

Norton AntiVirus cannot create a Boot Disk for all hard drives. You should always test your Norton AntiVirus Emergency Boot Disk to make sure that it works.

To test your Norton AntiVirus Emergency Boot Disk:

1. Click Start on the Windows taskbar, click Shut Down, select Shut Down Your Computer, and click OK.
2. Turn off the power.
3. Insert the Norton AntiVirus Emergency Boot Disk (Disk 1) in the A: drive, then restart your computer. Ignore the Norton AntiVirus Rescue text message that appears.
4. Type C: and press Enter to change to your hard drive.

   If the DOS prompt appears on screen (for example, C:\>), the Norton AntiVirus Emergency Boot Disk works properly. If the DOS prompt doesn’t appear, the Norton AntiVirus Emergency Boot Disk doesn’t work properly.

   Your Norton AntiVirus Emergency Boot Disk doesn’t work? See “My Norton AntiVirus Emergency Boot Disk doesn’t work,” on page 135.
5. Slide open the plastic tab on the back of the disk to write-protect it. This prevents you from accidentally changing the data stored on the disks.

If you didn’t create Rescue Disks

If you didn’t create Rescue Disks during installation, create them now. You need three 1.4 MB floppy disks and three disk labels.

To create Rescue Disks:

1. On the Windows taskbar, click Start, point to Programs, point to the Norton AntiVirus group, then click Rescue Disk.
2. Follow the on-screen instructions.
3. Test your Norton AntiVirus Emergency Boot Disk. See “Testing the Norton AntiVirus Emergency Boot Disk” on this page.

Uninstalling Norton AntiVirus for Windows 95

To uninstall Norton AntiVirus:

- On the Windows taskbar, click Start, point to Programs, point to the Norton AntiVirus group, then click Uninstall Norton AntiVirus.

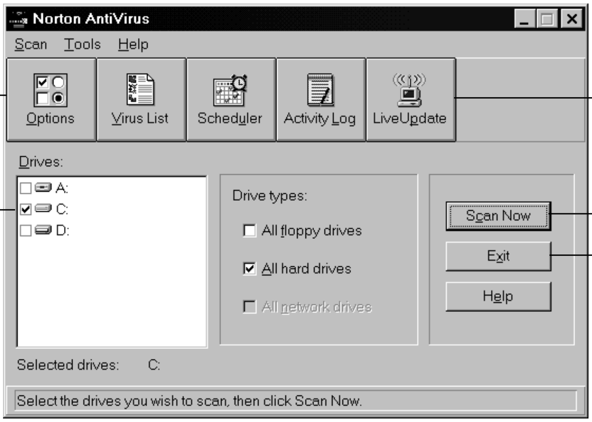
Quickstart

To start Norton AntiVirus:

- Click Start on the Windows taskbar, point to Programs, point to the Norton AntiVirus group, and click Norton AntiVirus.

  The Norton AntiVirus for Windows 95 main window appears.

Figure 1 Norton AntiVirus main window



□ A:
☑ C:
□ D:

□ All floppy drives
☑ All hard drives
□ All network drives

Selected drives: C:

Select the drives you wish to scan, then click Scan Now.

Scan a specific folder or file

Check drives you want to scan for viruses

Update virus definitions automatically

Start a virus scan

Exit Norton AntiVirus

To scan one or more drives to determine if your computer is infected by viruses:

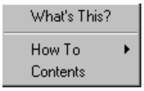
- In the Norton AntiVirus main window, check specific drives to scan in the Drives list box and click Scan Now.

To scan a specific file or folder:

- In the Norton AntiVirus main window, choose FILE from the Scan menu.
- In the Norton AntiVirus main window, choose FOLDERS from the Scan menu.

To get help while using Norton AntiVirus:

1. Position the mouse pointer over an option and click the right mouse button to display the pop-up context menu.
2. Choose one of the following from the context menu:



   - What's This? for a brief description of the option.
   - How To to display menu of procedural help choices.
   - CONTENTS to display the table of contents for the entire help system.

If you performed a complete installation and accepted the recommended options, Auto-Protect and Startup scans are already enabled and a scan of your hard disks is scheduled to run automatically once per week.

To make sure Auto-Protect is enabled:

1. Click Options in the Norton AntiVirus main window.
2. Click the Auto-Protect tab.
3. Check Load Auto-Protect At Startup.
4. Click OK.

To make sure Startup scans are enabled:

1. Click Options in the Norton AntiVirus main window.
2. Click the Startup tab.
3. Check the Memory, Master Boot Record, Boot Records, and System Files options in the What To Scan group box.
4. Click OK.

Making sure you’re protected

To keep your computer free of viruses, follow these rules:

- Update your virus definitions files monthly so that you maintain maximum protection against newly identified viruses. See Chapter 4, “Keeping up with new viruses,” on page 67 for directions.
- Scan all hard disk drives at least once per week to verify they are virus-free.
- Scan all new files and floppy disks before first use.

- Create a Norton AntiVirus rescue disk set, which you use to restore a damaged hard disk and recover from certain boot viruses. See "Creating a rescue disk set," on page 42 for more information.
- Make periodic backups of your hard disk.
- Buy legal copies of all software you use and make write-protected backup copies.

About Norton AntiVirus 1

Norton AntiVirus for Windows 95 is the most sophisticated and powerful product available to safeguard your computer from virus infection, no matter what the source. You are protected from viruses that spread from hard or floppy disks, viruses that travel across networks, and even viruses that are transmitted across the Internet.

Is my computer protected against viruses?

When you install Norton AntiVirus and accept the preset options, your computer is safe. As part of the installation, your computer is scanned for viruses. After the installation, Norton AntiVirus automatic protection features continually safeguard your computer while you work. If a virus is ever found, Norton AntiVirus guides you through the process of eliminating it.

If computers are a mystery to you, don't worry. The Norton AntiVirus preset options balance efficiency with maximum protection; you do not need to change anything. Simply install Norton AntiVirus and you are immediately protected from computer viruses.

Here's what Norton AntiVirus does automatically:

- Checks system files and boot records for viruses at system startup.
- Checks programs for viruses at the time you use them.
- Scans your computer for viruses once per week.
- Monitors your computer for activity that might indicate the work of a virus in action.
- Checks floppy disks for boot viruses when you use them.

Here's what you can do with Norton AntiVirus:

- Scan specific files, folders, or entire drives for viruses.
- Schedule virus scans to run at predetermined times.
- Update virus definitions files monthly.
- Customize Norton AntiVirus protection to match your risk level of virus infection.

What is a computer virus?

A computer virus is, simply, a computer program written by an ill-intentioned programmer. A virus program is designed in such a way that, when run, it attaches a copy of itself to another computer program. Thereafter, whenever the infected program is run, the attached virus program is activated and attaches itself to yet other programs. For example, a computer virus, which your computer may get by running an infected program from a borrowed floppy disk, infects other programs on your computer. A computer virus, like a biological virus, lives to replicate.

In addition to replicating, some computer viruses are programmed specifically to damage data by corrupting programs, deleting files, or even reformatting your entire hard disk. Most viruses, however, are not designed to do serious damage; they simply replicate or display messages.

Viruses can only infect files and corrupt data. They do not infect or damage hardware, such as keyboards or monitors. Though you may experience strange behaviors such as screen distortion or characters not appearing when typed, a virus has, in fact, merely affected the programs that control the display or keyboard. Your disks themselves are not physically damaged, just what's stored on them.

Computer viruses are classified by their targets, the items they infect:

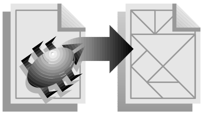
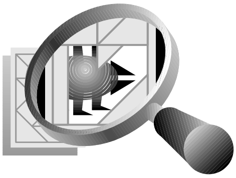
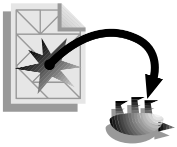
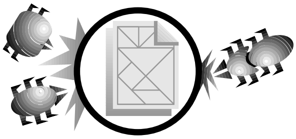
- Program viruses: These viruses infect executable files, such as word processing, spreadsheet, computer game, or operating system programs.
- Boot viruses: Some viruses can infect disks by attaching themselves to special programs in areas of your disks called boot records and master boot records. These areas contain the programs your computer uses to start up.
- Macro viruses: In many word processing and spreadsheet applications, you can record a macro that stores a series of actions. Later, you can run the macro and automatically repeat the same actions. Macro viruses infect data files with macro capabilities. For example, Microsoft Word document and template files are susceptible to macro virus attacks.

Virus infection cycle

There are three stages in the life of computer viruses: infection, detection, and recovery. In the infection stage, a virus infects a file in your computer. In the detection stage, the virus is identified and isolated. In the recovery stage, the virus is eliminated. Unless the virus is eliminated, it continues to infect other files and possibly damage data on your disks. Table 1-1, “Details of the virus life cycle,” on page 20 details each stage.

Norton AntiVirus is the most effective tool available to break this virus infection cycle. With Norton AntiVirus and its automatic protection features, you can prevent viruses from ever infecting your computer in the first place.

Table 1-1 Details of the virus life cycle

Infection 	**Source**	Reused floppy disks from unknown sources Disks from home or school Disks borrowed from friends Programs downloaded from BBSs or online services Software bargains (from non-reputable dealers) Re-shrink-wrapped or opened software Pirated software Preformatted floppy disks
	Infection	Boot from infected disk Reboot with infected floppy disk left in drive Run infected program Open infected document or spreadsheet
	Spread	Share disk or infected program Log on to network
Detection 	**Observation**	Strange system behavior Files missing or programs not working
	Utility	Virus detected by antivirus software
Recovery 	**Cleanup**	Reinstall programs from master disks Repair files with antivirus software Restore from uninfected backup
	Followup	Rescan all files to find source of infection Scan all floppy disks to find source of infection Discard backups that may be infected Increase virus protection for a while
Prevention 	Use Norton AntiVirus to prevent virus infection	

How Norton AntiVirus protects you

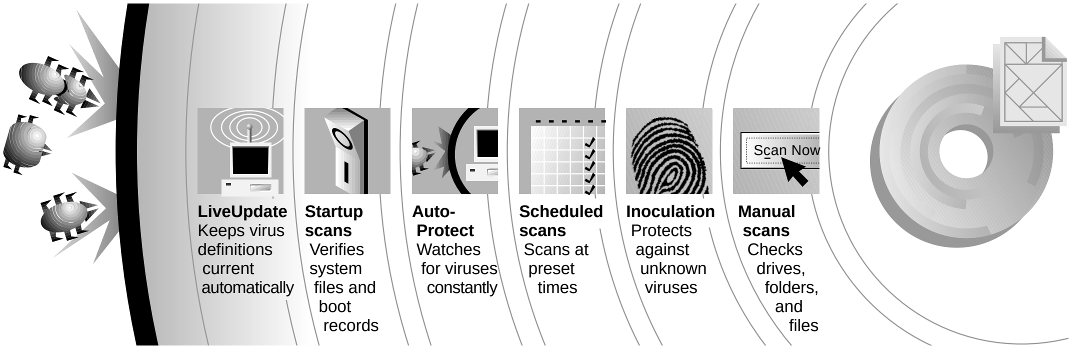
All computer viruses, irrespective of their targets, fall naturally into two groups:

- Known viruses: A known virus is one that has been identified. Symantec engineers work around the clock tracking reported outbreaks of computer viruses to identify new viruses. Once identified, information about the virus (a virus signature) is stored in a virus definitions file. When Norton AntiVirus scans your disks and files for viruses, it is searching for these telltale virus signatures. If an item is found that has been infected by one of these viruses, Norton AntiVirus has the tools to eradicate the virus automatically.

  Each time a new virus is discovered, its virus signature must be added to the virus definitions files. For this reason, you should update your virus definitions file regularly (a new file is available monthly from Symantec) so that Norton AntiVirus has the information it needs to find all known viruses. See Chapter 4, “Keeping up with new viruses,” on page 67 for instructions on getting the latest virus definitions files.
- Unknown viruses: An unknown virus is one that does not yet have a virus definition. Norton AntiVirus detects unknown viruses by monitoring activity on your computer for behaviors that viruses typically perform when replicating or attempting to damage files. It also looks for programs that have been modified without your knowledge. When a suspicious activity is detected, Norton AntiVirus prevents the action from continuing. If it detects a modified program, Norton AntiVirus prevents the program from running and takes corrective action.

Symantec engineers have developed several complementary technologies to keep your computer virus-free. Figure 1-1, “Norton AntiVirus technologies,” illustrates how the Norton AntiVirus technologies work together to detect, eliminate, and prevent viruses—whether known or unknown—from gaining entry to your computer.

Figure 1-1 Norton AntiVirus technologies

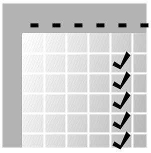

LiveUpdate
Keeps virus definitions current automatically
Startup scans
Verifies system files and boot records
Auto-Protect
Watches for viruses constantly
Scheduled scans
Scans at preset times
Inoculation
Protects against unknown viruses
Manual scans
Checks drives, folders, and files
Scan Now

The scanner, which examines program files for the signatures of known viruses, is the heart of Norton AntiVirus protection. It searches for virus signatures when you initiate manual scans, schedule scans to run at specific times, during startup scans that run automatically every time you start your computer, and by the Auto-Protect feature every time a file is used. The scanner verifies also that files protected by inoculation have not been altered by the work of an unknown virus. Auto-Protect, in addition to checking files for known viruses, uses its Virus Sensor technology and virus-like activity monitors to make sure that unknown viruses are neither infecting your computer nor damaging data during the course of normal operation.

Manual scans

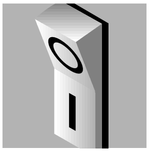
Use the Scan Now button in the Norton AntiVirus main window to initiate manual scans. These scans detect known viruses in specific files, folders, or drives on your computer. For information on how to scan files, folders, or drives, see "Scanning for viruses," on page 31.

Scheduled scans



Scheduled scans are manual scans that run automatically at predetermined times. These scans supplement other automatic protection features to ensure that your computer is virus-free. As part of the Norton AntiVirus installation, a scan of your computer is scheduled to run automatically once per week. For information on scheduling scans, see "Scheduling virus scans," on page 43.

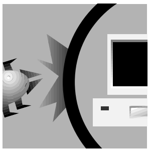
Startup scans



The first wave of defense against virus attacks are special scans that occur automatically each time your computer starts up. These scans catch viruses that infect the files and boot records your computer uses to ready itself for work. Startup scans are a vital part of virus protection because they make sure that your computer is virus-free each time you start it up.

The startup scan is turned on during installation, unless you specifically turn it off. For information on customizing startup scans, see "Customizing startup protection," on page 98.

Auto-Protect



Auto-Protect, the Norton AntiVirus automatic protection feature, scans program files, documents, and document template files for viruses whenever they are used. Auto-Protect also defends your computer from viruses by monitoring computer activity for virus-like behaviors (such as an attempted format of a hard disk) and warning you so you can stop them from occurring. In addition, Auto-Protect includes a sophisticated unknown virus detection component called Virus Sensor, which notifies you when a virus tries to attach itself to a program file.

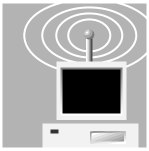
Auto-Protect is already turned on after installation, unless you specifically turn it off. For information on customizing Auto-Protect and turning the Virus Sensor on, see "Customizing automatic protection," on page 91.

Inoculation

Once you've scanned your disks to verify that your files are free of viruses, inoculation technology makes sure they stay virus-free. When you inoculate a file, Norton AntiVirus records critical information about it (similar to taking a fingerprint) in a special file designed specifically to store this inoculation data. Inoculation does not modify your original file in any way.

On subsequent scans—including manual scans, scheduled scans, and Auto-Protect scans—Norton AntiVirus compares a file's current fingerprint to its stored fingerprint. You are alerted if there are any changes that could indicate the presence of a virus. System files and boot records are inoculated automatically as part of your Norton AntiVirus installation. For information on inoculating program files, see "Inoculating files," on page 36 and "Customizing inoculation," on page 100.

Virus definitions files



Virus definitions files contain information that Norton AntiVirus uses during scans to detect known viruses. Norton AntiVirus depends on up-to-date information. Each time a new virus is discovered, its virus signature must be added to a virus definitions file. You should update your virus definitions files regularly so that Norton AntiVirus has the information it needs to find all known viruses.

New virus definitions files are available monthly from Symantec at no charge. If you have a modem or an Internet connection, Norton AntiVirus can update your virus definitions files for you automatically. See "Automatically updating virus definitions," on page 67 for information on how to receive the latest definitions.

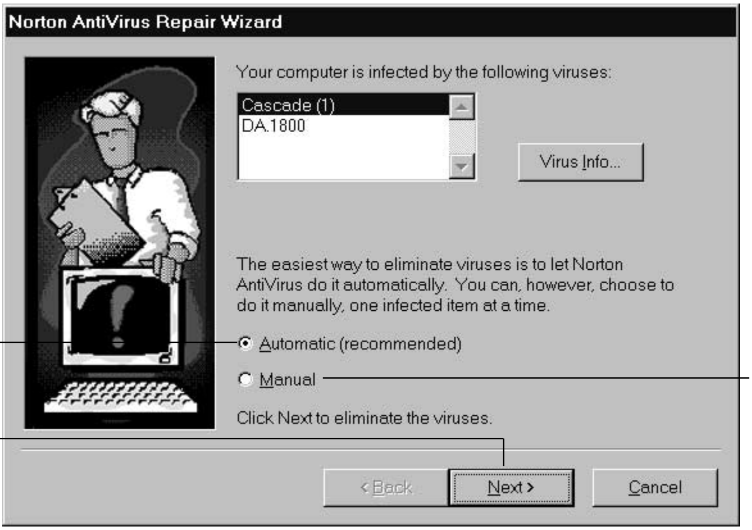
How Norton AntiVirus warns you

Norton AntiVirus warns you of possible virus infection in three different ways, depending upon how the virus was detected:

- Virus detected during manual or scheduled scans (see Figure 1-2).
- Viruses detected by Auto-Protect (see Figure 1-3).
- Viruses detected during startup scans.

If a virus is detected during a manual or scheduled scan, the Norton AntiVirus Repair Wizard appears so you can eliminate the virus automatically. Figure 1-2 shows the opening panel of the Repair Wizard.

Figure 1-2 Norton AntiVirus Repair Wizard



Your computer is infected by the following viruses:

Cascade (1)
DA.1800

The easiest way to eliminate viruses is to let Norton AntiVirus do it automatically. You can, however, choose to do it manually, one infected item at a time.

● Automatic (recommended)

○ Manual

Click Next to eliminate the viruses.

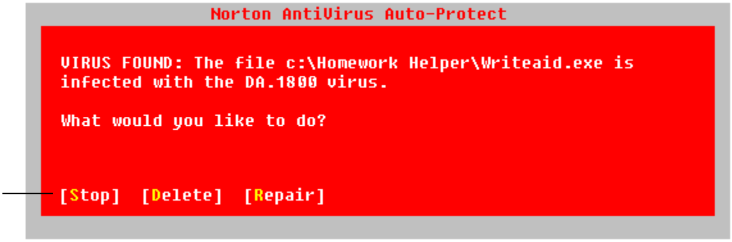
Norton AntiVirus eliminates all viruses automatically

Click Next to start the virus elimination

Repair infected items one at a time

Norton AntiVirus Auto-Protect, which constantly monitors for viruses, immediately displays a Virus Alert dialog box whenever an event concerning viruses occurs. (See Figure 1-3 for an example of an Auto-Protect alert.) Each Virus Alert dialog box has buttons that let you remove the virus. See "Eliminating viruses detected during scans," on page 49 for instructions on how to use the Repair Wizard.

Figure 1-3 Auto-Protect alert



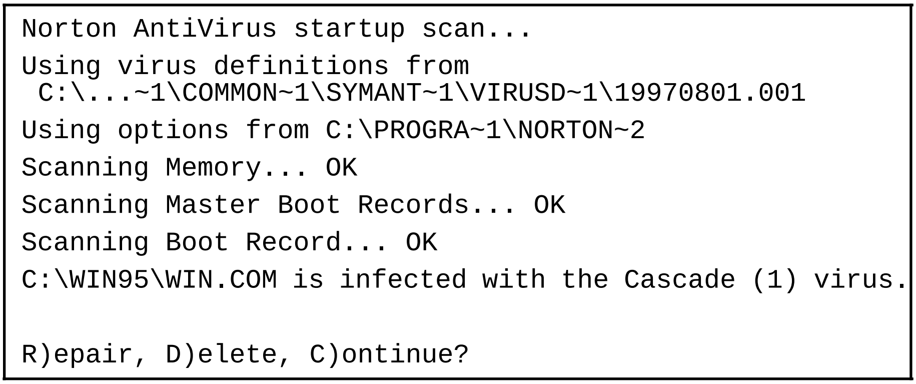
```
VIRUS FOUND: The file c:\Homework Helper\Writeaid.exe is
infected with the DA.1800 virus.

What would you like to do?
```

Actions you can take to respond to the alert

Norton AntiVirus startup scans run every time you start your computer. These scans catch viruses that infect system files and boot records. Because the scans run before Windows is loaded, alerts are simply reported as text on the screen. The alert prompts you to press a key to remove the virus.

Figure 1-4 Startup scan



```
Norton AntiVirus startup scan...
Using virus definitions from
 C:\...~1\COMMON~1\SYMANT~1\VIRUSD~1\19970801.001
Using options from C:\PROGRA~1\NORTON~2
Scanning Memory... OK
Scanning Master Boot Records... OK
Scanning Boot Record... OK
C:\WIN95\WIN.COM is infected with the Cascade (1) virus.

R)epair, D)elete, C)ontinue?
```

See “Eliminating viruses detected during startup scans,” on page 62 for instructions on what to do if you receive an alert during a startup scan.

Using Norton AntiVirus 2

A virus can become active only if you start (or attempt to start) your computer from a disk infected with a boot virus, if you run an infected program, or open an infected document or template.

Tips to avoid viruses

Some precautions you can take to minimize your virus risk:

- Make sure automatic protection is turned on at all times. Automatic protection is already set up for you when you install Norton AntiVirus using the preset options. For more information, see "Customizing automatic protection," on page 91 and "Customizing startup protection," on page 98.
- Perform a manual scan (or schedule a scan to occur automatically) of your hard disks once per week. These scans supplement automatic protection and confirm that your computer is virus-free. A scan is already scheduled to run automatically once per week when you install Norton AntiVirus using the preset options. See "Scanning for viruses," on page 31 and "Scheduling virus scans," on page 43.
- Scan all floppy disks before first use. See "Scanning for viruses," on page 31 for directions.
- Update your virus definitions files every month. See "Automatically updating virus definitions," on page 67 for directions.
- Create and maintain a Norton AntiVirus rescue disk set to facilitate recovery from certain boot viruses. See "Creating a rescue disk set," on page 42 for directions.
- Make periodic backups of your hard disk.
- Buy legal copies of all software you use and make write-protected backups.

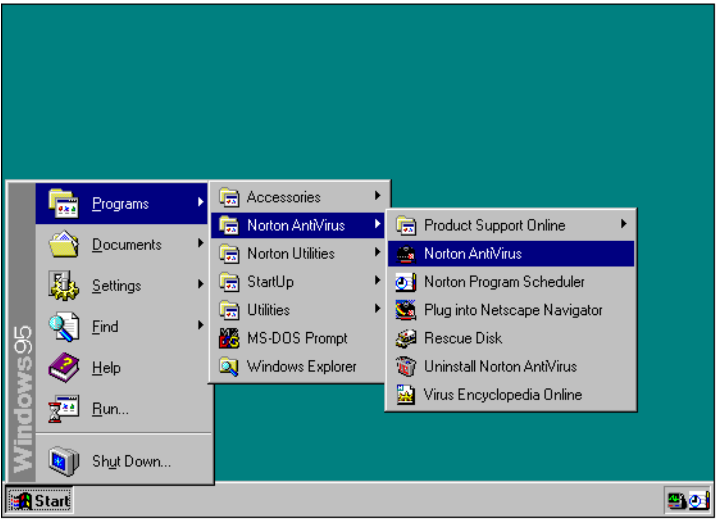
Starting and exiting Norton AntiVirus

You use the Norton AntiVirus main window to initiate scans for viruses, schedule scans that run automatically, view or change configuration options, or update virus definitions files. Auto-Protect is always running (see "Enabling and disabling Auto-Protect," on page 33 for information about Auto-Protect).

To start Norton AntiVirus:

- Click Start on the Windows taskbar, choose Programs, choose the Norton AntiVirus group, and, finally, click Norton AntiVirus (Figure 2-1). The Norton AntiVirus for Windows main window appears (see Figure 2-2).

Figure 2-1 Starting Norton AntiVirus

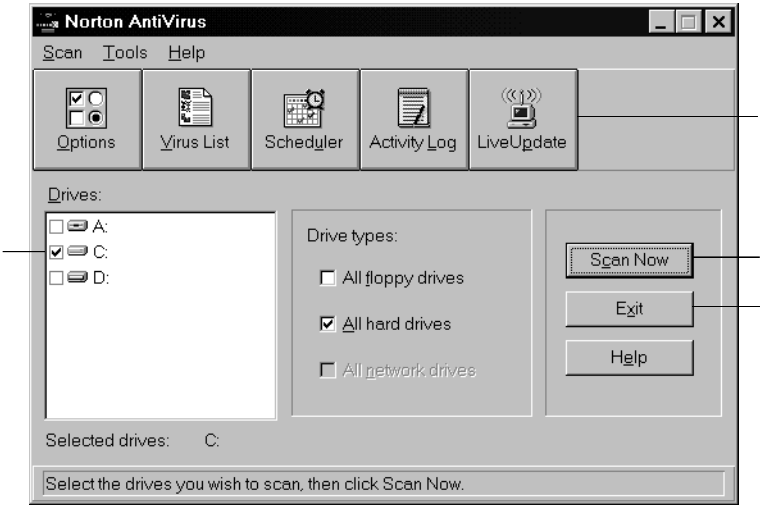


Click Start to choose Norton AntiVirus

To exit Norton AntiVirus:

- Click Exit in the Norton AntiVirus main window.

Figure 2-2 Norton AntiVirus main window



Drives:
□ A:
☑ C:
□ D:

Drive types:
□ All floppy drives
☑ All hard drives
□ All network drives

Selected drives: C:

Select the drives you wish to scan, then click Scan Now.

Update virus definitions automatically

Check the drives you want to scan for viruses

Start a virus scan

Exit Norton AntiVirus

Getting help

Online help is provided for all capabilities of Norton AntiVirus. You can get help on concepts, definitions, and procedures by:

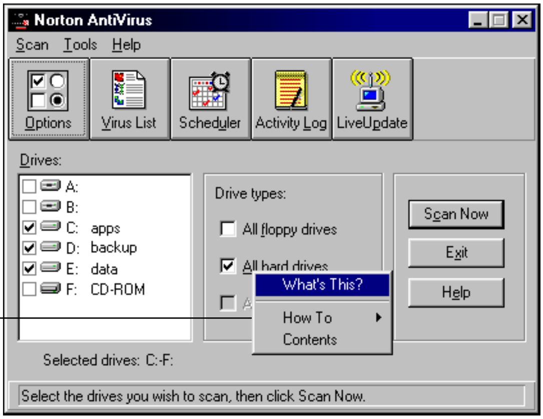
- Clicking the right mouse button on items in a dialog box.
- Using commands on the Help menu.
- Clicking the Help button in a dialog box.

The help system includes a table of contents, an extensive topics index, and a glossary. From the help window you can search for, print, annotate, and establish bookmarks for specific help topics. You can also access context-sensitive help for any option in Norton AntiVirus.

To access context-sensitive help:

1 Position the mouse pointer over an option and click the right mouse button to display the help pop-up menu.

Figure 2-3 Right button help menu



☐ A:
☐ B:
☑ C: apps
☑ D: backup
☑ E: data
☐ F: CD-ROM

☐ All floppy drives
☑ All hard drives

Selected drives: C:-F:

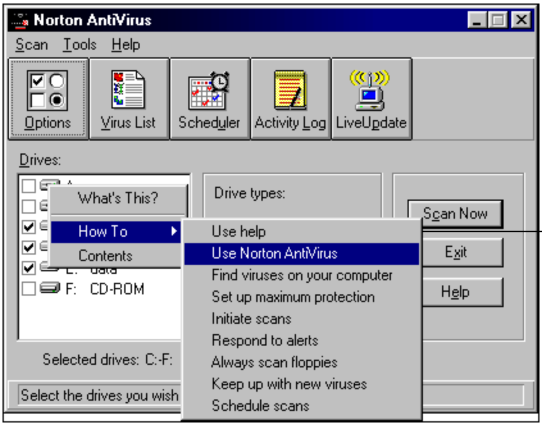
Select the drives you wish to scan, then click Scan Now.

Right button help menu

2 Choose one of the following from the pop-up menu:

- WHAT'S THIS? shows a brief description of the option.
- HOW TO displays menu of procedural help choices related to the option (Figure 2-4).
- CONTENTS displays the table of contents for the entire help system.

Figure 2-4 How To help menu



☐ F: CD-ROM

Selected drives: C:-F:

Select the drives you wish

Select a step-by-step procedure

Another way to access context-sensitive help for an option in a dialog box is with the question mark icon in the title bar of any dialog box.

To get help about options:

1 Click the question mark icon in the right corner of the title bar of any dialog box.

A question mark appears next to the mouse pointer.

2 Click any option in the dialog box.

A brief explanation of the option pops up.

Scanning for viruses

You can initiate a virus scan at any time. As a general practice, scan your hard disks at least once a week or schedule a scan to occur automatically. Always scan floppy disks before you use them for the first time and always scan files downloaded from bulletin boards and other online services.

At the end of each scan, Norton AntiVirus reports its findings. If any problems are found, the Norton AntiVirus Repair Wizard appears so you can direct repairs (see "Eliminating viruses detected during scans," on page 49). After the problems are dealt with, as well as after a scan with no problems found, a scan summary details everything that happened during the scan.

TIP: The Norton AntiVirus preset options balance maximum protection with efficiency during scans. In most cases you do not need to change anything. You can, however, customize what is scanned and what to do if a virus is found. See "Customizing manual scan options," on page 75 for directions.

To scan one or more drives:

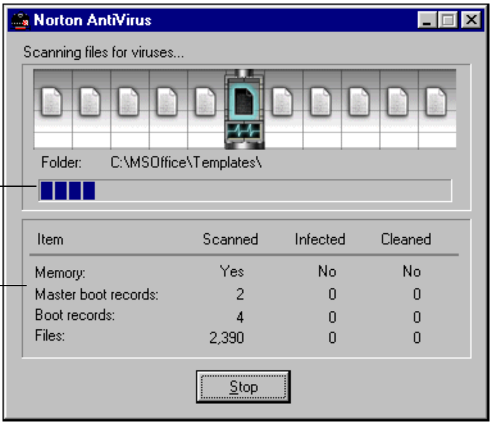
1 Start Norton AntiVirus.

2 In the Norton AntiVirus main window, check specific drives to scan in the Drives list box or select multiple drives by checking items in the Drive Types group box (see Figure 2-2).

3 Click Scan Now.

The Scan dialog box reports the progress of the scan.

Figure 2-5 Scan in progress



Scanning files for viruses...

Folder: C:\MSOffice\Templates\

Item	Scanned	Infected	Cleaned
Memory:	Yes	No	No
Master boot records:	2	0	0
Boot records:	4	0	0
Files:	2,390	0	0

Progress of the scan

Summary of scan progress

To scan an individual file:

1 In the Norton AntiVirus main window, choose FILE from the Scan menu.

2 Select the file you want to scan and click OK.

To scan an individual folder:

1 In the Norton AntiVirus main window, choose FOLDERS from the Scan menu.

2 Select the folder you want to scan.

3 Click Scan.

Norton AntiVirus is preset to scan program files, documents, and document templates only during a scan, because these are the only types of files from which viruses spread. Occasionally, such as after a virus attack, you may want to scan all files to make sure that a file that may not appear as a regular program file gets scanned as well.

To scan all files, regardless of type:

1 In the Norton AntiVirus main window, click Options.

2 Click the Scanner tab (Figure 2-6).

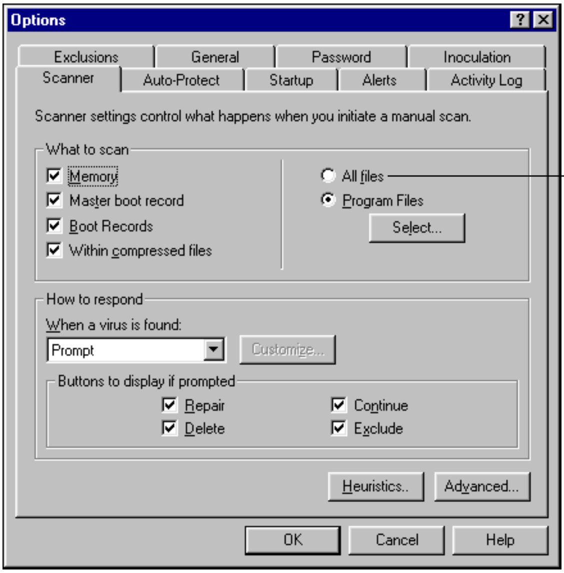
3 Select the All Files option.

4 Click OK to return to the Norton AntiVirus main window.

5 Select the drives to scan and click Scan Now.

See “Selecting which files to scan,” on page 80 for more information about selecting Program Files or All Files for scanning.

Figure 2-6 Scanner options tab



Scanner settings control what happens when you initiate a manual scan.

What to scan

☑ Memory
☑ Master boot record
☑ Boot Records
☑ Within compressed files

○ All files
● Program Files

How to respond

When a virus is found: Prompt

Buttons to display if prompted

☑ Repair
☑ Delete
☑ Continue
☑ Exclude

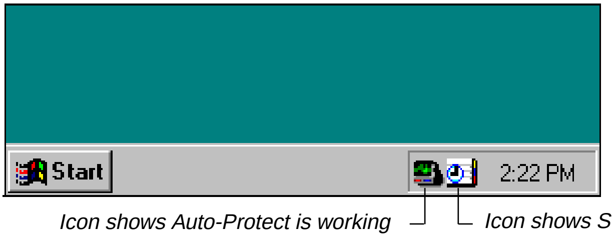
Scan all files, regardless of type

Enabling and disabling Auto-Protect

Norton AntiVirus is preset to load Auto-Protect—the automatic virus protection technology—whenever you start your computer. The Norton AntiVirus Auto-Protect icon appears on the Windows taskbar (Figure 2-7). If the Auto-Protect icon does not appear on the Windows taskbar, either Auto-Protect is not loaded or Auto-Protect is configured not to display an icon on the taskbar.

Generally, you should not disable Auto-Protect. It is your best protection against virus attack. There are only a few situations when you might want to disable Auto-Protect. For example, sometimes you are told to disable anti-virus protection before installing a new program.

Figure 2-7 Windows taskbar



Icon shows Auto-Protect is working

Icon shows Scheduler is running

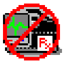
To disable automatic protection temporarily:

1. Double-click the Auto-Protect icon on the Windows taskbar (Figure 2-7).

   The Norton AntiVirus Auto-Protect dialog box appears (Figure 2-8).

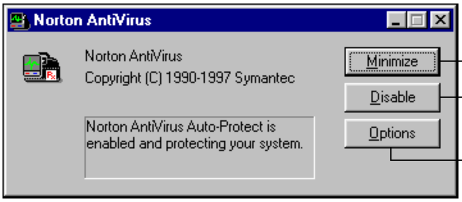
2. Click Disable.

   The button changes to Enable and the icon in the taskbar changes to

3. Click Minimize to close the Norton AntiVirus Auto-Protect dialog box.

Figure 2-8 Auto-Protect dialog box



Norton AntiVirus
Copyright (C) 1990-1997 Symantec

Norton AntiVirus Auto-Protect is enabled and protecting your system.

Click to minimize Auto-Protect as an icon on the taskbar

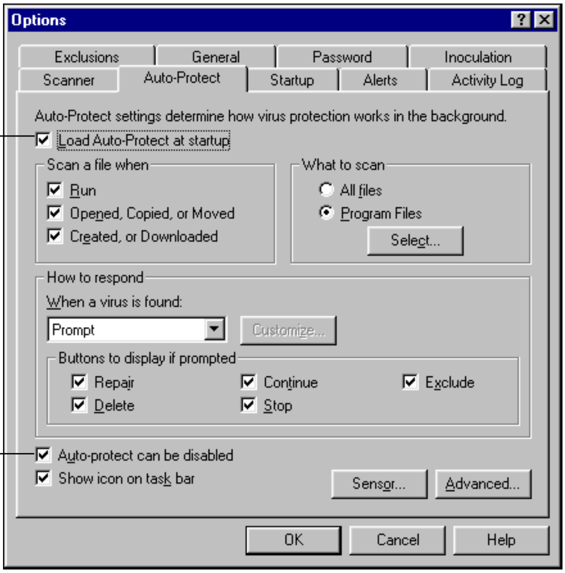
Click to Disable or Enable Auto-Protect

Click to configure Auto-Protect

To load Auto-Protect every time you start your computer:

1. Start Norton AntiVirus.
2. Click Options in the Norton AntiVirus main window (see Figure 2-2).
3. Click the Auto-Protect tab.

Figure 2-9 Setting Auto-Protect options



Auto-Protect settings determine how virus protection works in the background.

☑ Load Auto-Protect at startup

Scan a file when
- ☑ Run
- ☑ Opened, Copied, or Moved
- ☑ Created, or Downloaded

What to scan
- ○ All files
- ● Program Files

How to respond

When a virus is found: Prompt

Buttons to display if prompted
- ☑ Repair
- ☑ Delete
- ☑ Continue
- ☑ Stop
- ☑ Exclude

☑ Auto-protect can be disabled

☑ Show icon on task bar

Check to make sure Auto-Protect loads at system startup

Check so the Auto-Protect icon shows on the taskbar

4 Check Load Auto-Protect at Startup and click OK.

Norton AntiVirus enables Auto-Protect immediately and every time your computer starts up thereafter.

Bypassing startup protection

Startup scans, which ensure that the files your computer uses to start up are not infected, are a vital part of protecting your computer against viruses. Although it’s not recommended, there may be times when you don’t want Norton AntiVirus to scan for viruses during system startup. For example, you may be trying to solve a system startup problem or a configuration file conflict.

To bypass system startup scans:

- Press and hold the specified bypass keys during the entire boot process. By default, they are the two Alt keys.

Bypassing system startup scans applies only to a single startup. For information on what bypass keys are, specifying what is scanned at startup, and preventing a startup scan from being bypassed, see “Customizing startup protection,” on page 98.

Inoculating files

If you install Norton AntiVirus using the preset options, inoculation protection is set up for boot records and system files. You don't have to do anything further. In a high-risk environment, however, you may choose to inoculate all program files for added protection.

When you inoculate a program file or boot record, Norton AntiVirus records critical information about it (similar to taking a fingerprint) in a special data file referred to as the inoculation file. Separate inoculation files are created for each drive on which you inoculate files. Inoculation doesn't change a file or boot record. Only program files (including system files) and startup disk boot records can be inoculated because they are the parts of your system from which viruses generally spread.

On subsequent scans—a manual scan, a scheduled scan, or an Auto-Protect scan—Norton AntiVirus checks your files and boot records against their stored fingerprints. You are alerted if there are any changes that could indicate the presence of an unknown virus.

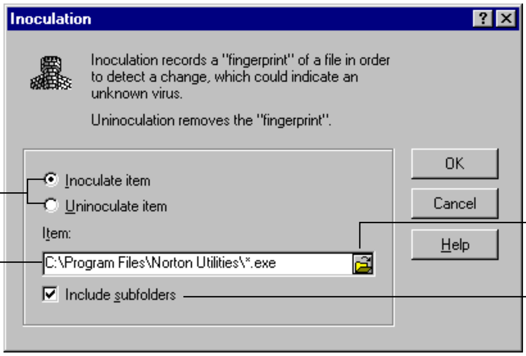
If you are in a high-risk environment and choose to inoculate program files in addition to boot records and system files, there are two ways to proceed:

- You can inoculate individual files or folders at any time using the INOCULATION command from the Tools menu in the Norton AntiVirus main window.
- You can inoculate program files, system files, and boot records during a manual scan. See "Customizing inoculation," on page 100 for information.

To inoculate individual files or folders:

1 In the Norton AntiVirus main window, choose INOCULATION from the Tools menu.

Figure 2-10 Inoculation dialog box



Inoculation records a "fingerprint" of a file in order to detect a change, which could indicate an unknown virus.

Uninoculation removes the "fingerprint".

● Inoculate item
○ Uninoculate item

Item: C:\Program Files\Norton Utilities*.exe

☑ Include subfolders

Inoculate or uninoculate the selected item

File or group of files to inoculate

Click the browse button to choose a file from a list

Inoculate files in subfolders too

2 Select Inoculate Item.

3 In the Item text box, do one of the following:

- Type the pathname for the file, group of files, folder, or drive that you want to inoculate.

  Just enter the folder name to inoculate all files in the folder. For example, type `C:\WINDOWS\COMMAND` to inoculate all files in your DOS folder.

  You can also use a wildcard to specify a group of files. For example, type `C:\WINDOWS\COMMAND\*.COM` to inoculate only .COM files in your DOS folder.

- Click the browse button to choose a single file from a list, then click Open.

TIP: When you inoculate items, Norton AntiVirus is storing inoculation data about the item. You must also make sure that inoculation protection is turned on so that the items are checked for inoculation changes during scans. Use the check boxes on the Options Inoculation tab to turn inoculation on or off. See “Customizing inoculation,” on page 100 for directions to turn inoculation on.

4 If the item is a folder, check Include Subfolders to inoculate files in all descending folders.

5 Click OK.

To inoculate files and boot records during a scan:

1 Make sure inoculation protection is turned on.

Use the check boxes on the Options Inoculation tab to turn inoculation on or off. You can choose boot records and system files as well as program files. You can only inoculate boot records and system files on your startup drive. See “Customizing inoculation,” on page 100 for directions to turn inoculation on.

2 Scan the files, folders, or drives that you want to inoculate.

All files are scanned automatically to make sure they are not infected before they are inoculated. See “Scanning for viruses,” on page 31 for information on how to initiate scans.

Reinoculating files and boot records

Reinoculating a program file or boot record creates a new fingerprint for the item to replace the previous data in the inoculation file.

You should reinoculate program files when you:

- Modify the program file in some way, such as upgrading to a new version.
- Move the file to a new location.

You should reinoculate boot records and system files when you:

- Install a new operating system on your hard disk.
- Repartition your hard disk.

TIP: You should also remake your Norton AntiVirus rescue disk set when you repartition a drive or install a new operating system on your hard disk. For more information, see “Creating a rescue disk set,” on page 42.

To reinoculate an item:

- Follow the procedure titled "To inoculate individual files or folders:," on page 37 to reinoculate files.

If Norton AntiVirus generates an inoculation alert, such as when you have upgraded an application but haven't yet reinoculated the program, you can simply click Inoculate in the alert dialog box. See "Responding to Auto-Protect inoculation alerts," on page 60 for more information.

To reinoculate from an alert box, Norton AntiVirus must be configured to prompt you when it detects inoculation changes. For more information, see "Customizing inoculation," on page 100.

Uninoculating files or folders

There are situations when you may want to uninoculate a file or folder. For example, you may uninoculate a folder before upgrading the programs in the folder to prevent inoculation change alerts when you later scan the folder. Uninoculating removes the inoculation data from the inoculation file.

You cannot uninoculate system files and boot records. However, you can configure Norton AntiVirus to not check for inoculation changes in these areas. See "Customizing inoculation," on page 100.

To uninoculate files:

1. Choose INOCULATION from the Tools menu in the Norton AntiVirus main window.
2. Select Uninoculate Item.
3. In the Item text box, do one of the following:
   - Type the pathname for the file, group of files, folder, or drive.

     You can use a wildcard to specify a group of files. For example, type `C:\WINDOWS\COMMAND\*.COM` to uninoculate all .COM files in your DOS folder.
   - Click the browse button to choose a single file from a list, then click Open.
4. If the item is a folder, check Include Subfolders to uninoculate files in all descending folders.
5. Click OK.

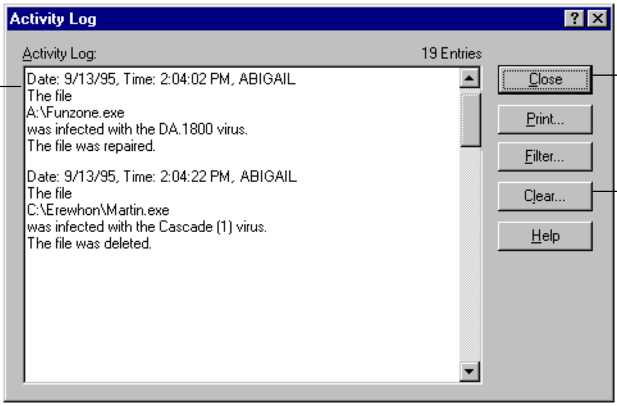
Viewing the Activity Log

The Activity Log file contains details of Norton AntiVirus activities, such as when problems were found and how they were resolved. For information on specifying what is stored in the Activity Log, see "Customizing the Activity Log," on page 88.

To view all entries in the Activity Log:

1 Click Activity Log in the Norton AntiVirus main window.

Figure 2-11 Activity Log



```
Date: 9/13/95, Time: 2:04:02 PM, ABIGAIL
The file
A:\Funzone.exe
was infected with the DA.1800 virus.
The file was repaired.

Date: 9/13/95, Time: 2:04:22 PM, ABIGAIL
The file
C:\Erewhon\Martin.exe
was infected with the Cascade (1) virus.
The file was deleted.
```

The entries are displayed in the list box

Activity Log options

2 Click Close to exit the Activity Log.

From the Activity Log dialog box you can also:

Print...

Click Print to print the Activity Log to a printer or a file. Only the entries currently displayed in the list box are printed. If you filter the Activity Log, only the filtered entries are printed.

Filter...

Click Filter to limit the display to specific types of events, such as all virus detections.

Clear...

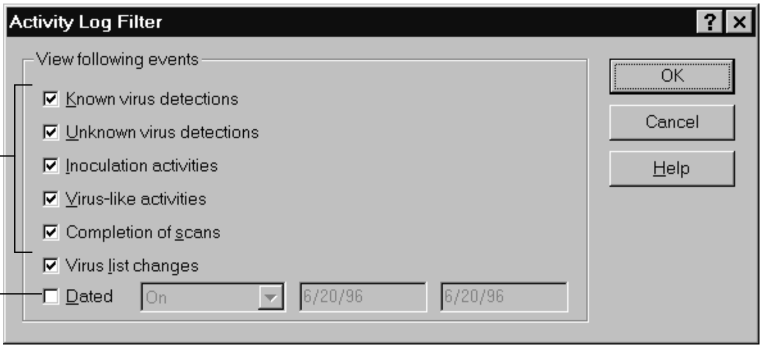
Click Clear to delete all of the entries in the Activity Log.

To filter the Activity Log entries:

1. Click Filter in the Activity Log dialog box (see Figure 2-11).

   The Activity Log Filter dialog box appears (Figure 2-12).

Figure 2-12 Activity Log Filter



View following events

☑ Known virus detections

☑ Unknown virus detections

☑ Inoculation activities

☑ Virus-like activities

☑ Completion of scans

☑ Virus list changes

☐ Dated On 6/20/96 6/20/96

Types of events to view

View events based on date of occurrence

2. Check the types of events you want listed. If no entries match your filter, a “No items to display” dialog box appears instead. In this case, the filter changes are ignored and the previous settings are restored.

   - Known Virus Detections: Displays information on known virus detections.
   - Unknown Virus Detections: Displays information on unknown virus detections.
   - Inoculation Activities: Displays information on files that have not been inoculated or have changed since inoculation.
   - Virus-like Activities: Displays information on virus-like activity detections.
   - Completion Of Scans: Displays information about when scans occurred. This option applies to manual and scheduled scans only.
   - Virus List Changes: Displays information about changes to the virus list.
   - Dated: Indicates the date or range of dates for displaying the selected events. Select an option in the Dated drop-down list box, then enter the date or dates to define the scope.

3. Click OK.

Creating a rescue disk set

A Norton AntiVirus rescue disk set is an important part of virus protection. It stores critical system information and the programs necessary to start your computer, and are necessary to recover from certain types of boot viruses. The rescue set is composed of the following disks:

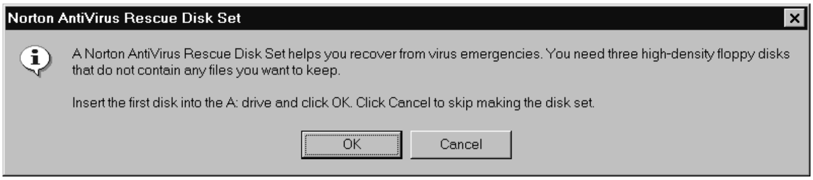
- Norton AntiVirus Emergency Boot Disk: Used to start your computer.
- Norton AntiVirus Program Disk: Used to scan for and remove viruses.
- Norton AntiVirus Definitions Disk: Virus definitions files used during scans.

When you installed Norton AntiVirus, you were given the opportunity to create a rescue disk set. If you did not do it then, do it now. You need three high-density floppy disks for the set.

To create a rescue disk set:

1 Click Start on the Windows taskbar, choose Programs, choose the Norton AntiVirus group, and click Rescue Disk.

Figure 2-13 Creating a rescue disk set



Norton AntiVirus Rescue Disk Set

A Norton AntiVirus Rescue Disk Set helps you recover from virus emergencies. You need three high-density floppy disks that do not contain any files you want to keep.

Insert the first disk into the A: drive and click OK. Click Cancel to skip making the disk set.

2 Insert a floppy disk in the A: drive and click OK.

The floppy disk will be formatted as part of the process. Don’t use floppy disks with files you need to keep.

3 Follow the prompts. You will be notified when to change floppy disks. The entire procedure will take a few minutes.

4 When the Norton AntiVirus rescue disk set is created, follow the instructions on the screen to label the disks, including the computer for which they were created and the date the set was made.

5 Write-protect the Norton AntiVirus rescue disks (slide open the plastic tab on the back of each disk) and store them in a safe place.

Scheduling virus scans

You can schedule virus scans that run unattended on either specific dates and times or at periodic intervals. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working. A scan is already scheduled to run automatically once per week when you install Norton AntiVirus using the preset options.

When you close the Scheduler, you can click Exit or Minimize. Make sure you click the Minimize button so that the Scheduler remains active. The Scheduler must be active before scheduled scans can run.

TIP: You can also use the Microsoft Plus! System Agent to schedule scans. See Appendix C, "Using command-line switches" on page 119 for information on running NAVW32.EXE, the Norton AntiVirus scanner.

To access the Scheduler, use one of the following methods:

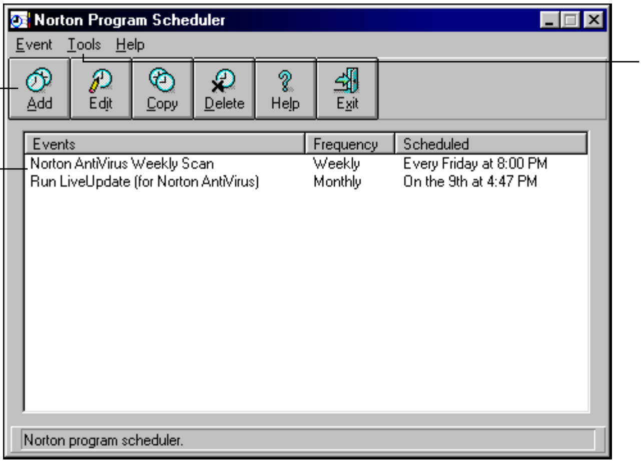
- Click Scheduler in the Norton AntiVirus main window.
- Choose NORTON PROGRAM SCHEDULER from the Windows Start menu.

If no events are already scheduled, the Edit, Copy, and Delete buttons are dimmed.

Figure 2-14 The Norton Program Scheduler

Click to schedule a scan

Events you schedule are listed here



Events	Frequency	Scheduled
Norton AntiVirus Weekly Scan	Weekly	Every Friday at 8:00 PM
Run LiveUpdate (for Norton AntiVirus)	Monthly	On the 9th at 4:47 PM

Norton program scheduler.

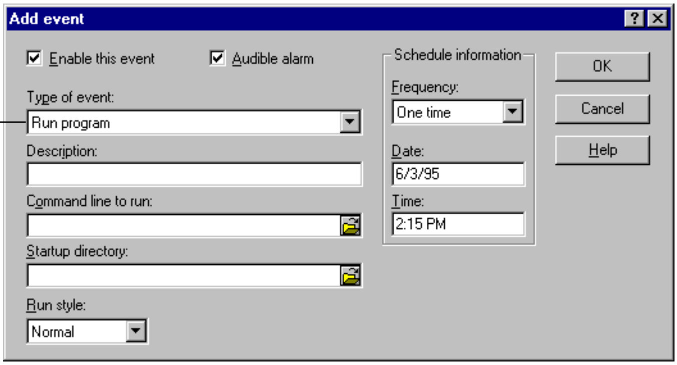
Choose Options from the Tools menu to make sure Scheduler loads with Windows

To schedule virus scans:

1 Click Add.

The Add Event dialog box appears so you can schedule any type of event.

Figure 2-15 Add event dialog box



Add event

☑ Enable this event ☑ Audible alarm

Type of event: Run program

Description:

Command line to run:

Startup directory:

Run style: Normal

Schedule information

Frequency: One time

Date: 6/3/95

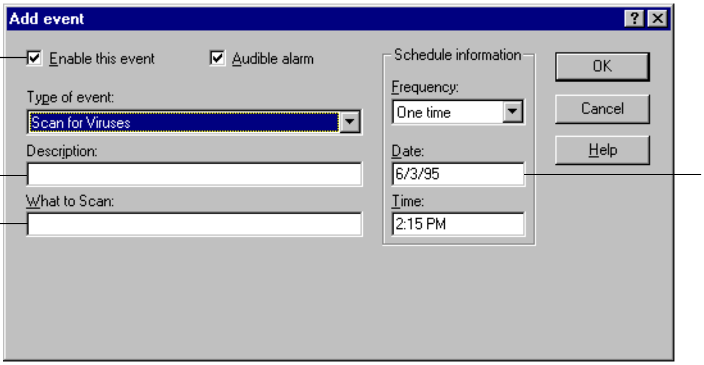
Time: 2:15 PM

Select Scan for Viruses from the drop-down list

2 Select Scan For Viruses in the Type Of Event drop-down list box.

The dialog box changes to accept information specific to a virus scan.

Figure 2-16 Add event dialog box with Scan for Viruses selected



Add event

☑ Enable this event ☑ Audible alarm

Type of event: Scan for Viruses

Description:

What to Scan:

Schedule information

Frequency: One time

Date: 6/3/95

Time: 2:15 PM

This must be checked for the scan to run

Helps you remember the purpose of the scan

Enter the items you want scanned

When the scan will occur

3 Check Enable This Event.

If you uncheck this option, the scan won't run.

4 Check Audible Alarm to hear a beep when the scan starts.

5 Type a brief description in the Description text box.

This text will appear in the events list in the Scheduler dialog box.

6 Type the drive letter or pathname for the drive, folder, or file you want scanned in the What To Scan text box.

NOTE: Do not leave the What To Scan text box blank. You must specify what to scan.

To specify your hard disk, type the drive letter followed by a colon.

```
C:
```

To specify more than one item to scan, use a space between items.

```
C: D:\Applications
```

If the path uses spaces, enclose the item in double quotes.

```
"C:\Rad Was Here\Hithere.exe"
```

You can use any of the NAVW32.EXE switches with Scheduler. See "NAVW32.EXE," on page 122 for a list of command-line switches.

7 Select how often you want the scan to occur in the Frequency drop-down list box.

8 Finish scheduling the scan by entering the correct time, day, or date information, if necessary.

9 Click OK. If prompted for confirmation, also click OK in the confirmation dialog box.

TIP: You can schedule any program to run or just display a message at a particular time. Simply select the Type Of Event in the drop-down list box and enter the requested information. The dialog box changes appropriately.

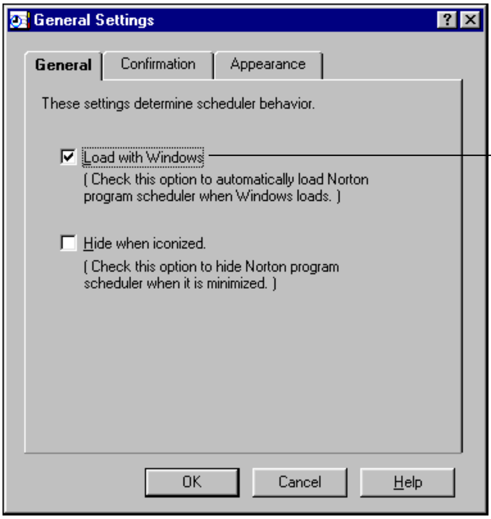
To make sure Scheduler loads when you start Windows:

1 Start Norton AntiVirus.

2 Click Scheduler in the Norton AntiVirus main window.

3 Choose OPTIONS from the Scheduler Tools menu.

Figure 2-17 Scheduler options settings



These settings determine scheduler behavior.

☑ Load with Windows
(Check this option to automatically load Norton program scheduler when Windows loads.)

□ Hide when iconized.
(Check this option to hide Norton program scheduler when it is minimized.)

Make sure this is checked so that Scheduler always loads when you start Windows

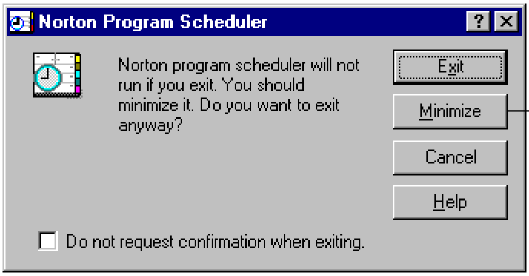
4 Make sure Load With Windows is checked on the General tab.

The Scheduler must be loaded in order to execute the scans you have scheduled.

To close the Scheduler:

1 Click Exit in the Scheduler main window.

Figure 2-18 Closing the Scheduler



Norton program scheduler will not run if you exit. You should minimize it. Do you want to exit anyway?

□ Do not request confirmation when exiting.

Click to close the Scheduler, but keep it active

2 Click Minimize.

The Scheduler remains active so that the scan can run at the time you specified.

The scans you schedule will run automatically. If your computer is turned off or the Scheduler is not loaded when a scan is scheduled to take place, you are notified that the scan was cancelled the next time the Scheduler loads.

To manage scheduled events:

From the Scheduler dialog box (see Figure 2-14) you can also:

Click Edit to make changes to a scheduled scan.

Click Copy to make a copy of a scheduled scan. This option is useful when you want to schedule a scan that is similar to one already on the list.

Click Delete to delete scheduled scans you no longer want.

Eliminating viruses 3

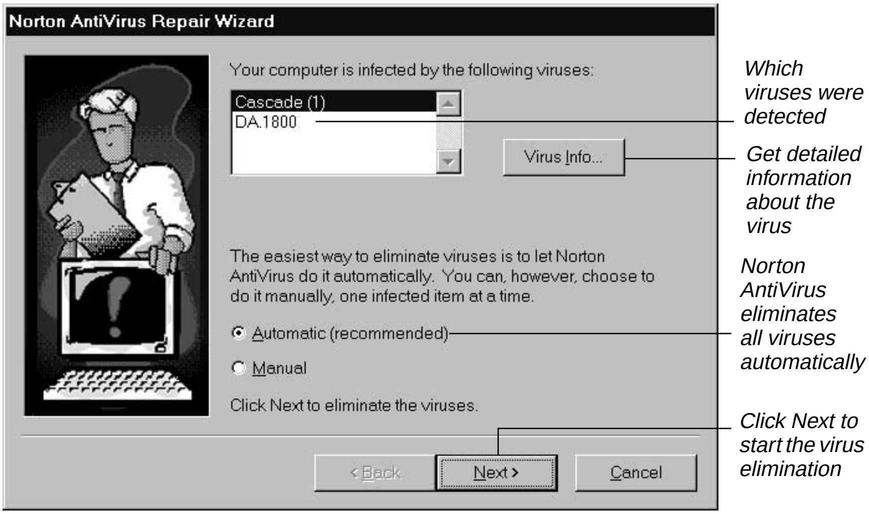
Norton AntiVirus warns you of possible virus infection in three different ways, depending upon how the virus was detected:

- Virus detected during manual or scheduled scans: The Norton AntiVirus Repair Wizard appears at the end of the scan to eliminate all viruses found automatically. See "Eliminating viruses detected during scans," on page 49.
- Viruses detected by Auto-Protect: Auto-Protect, which is constantly monitoring your computer for viruses, displays a virus alert immediately when an infected item is detected. The command buttons in the virus alert let you resolve the virus issue. See "Eliminating viruses detected by Auto-Protect," on page 54.
- Viruses detected during startup scans: Startup scans, which run when you first start up your computer, catch viruses that infect the files and boot records your computer uses to ready itself for work. You are prompted to press a key to eliminate the virus. See "Eliminating viruses detected during startup scans," on page 62.

Eliminating viruses detected during scans

If viruses are detected during a scan, the Norton AntiVirus Repair Wizard appears at the end of the scan (Figure 3-1). You can let Norton AntiVirus eliminate all viruses automatically or you can choose to eliminate the viruses manually, one item at a time.

Figure 3-1 Norton AntiVirus Repair Wizard



Your computer is infected by the following viruses:

The easiest way to eliminate viruses is to let Norton AntiVirus do it automatically. You can, however, choose to do it manually, one infected item at a time.

● Automatic (recommended)

○ Manual

Click Next to eliminate the viruses.

Which viruses were detected

Get detailed information about the virus

Norton AntiVirus eliminates all viruses automatically

Click Next to start the virus elimination

To eliminate all viruses automatically:

1 Scan a drive, folder, or file with Norton AntiVirus.

The Repair Wizard appears only if a virus is detected (Figure 3-1).

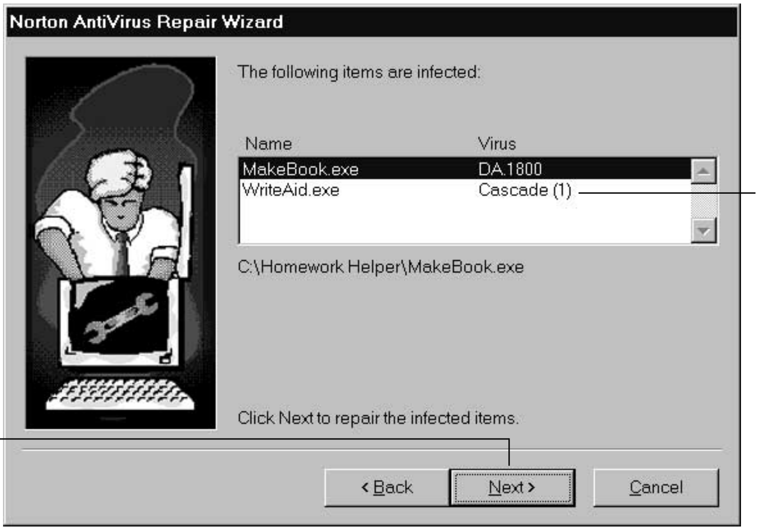
2 Select Automatic in the Norton AntiVirus Repair Wizard and click Next.

If you select Manual, see "To resolve virus issues manually, item by item:," on page 51 for directions.

3 Read each succeeding panel (Figure 3-2) to understand what Norton AntiVirus is doing, then click Next to continue.

The Repair Wizard will not take any action without asking permission first.

Figure 3-2 Which items are infected



Norton AntiVirus Repair Wizard

The following items are infected:

Name	Virus
MakeBook.exe	DA.1800
WriteAid.exe	Cascade (1)

C:\Homework Helper\MakeBook.exe

Click Next to repair the infected items.

Shows which items are infected

Click Next to begin the repair. The Repair wizard will not take any action without asking permission first

TIP: When the Repair Wizard finishes, the last panel summarizes what actions Norton AntiVirus performed. On this panel you can click More Info if you want details about the operations, or want to print a report about what was infected and repaired.

If you select Manual in the Norton AntiVirus Repair Wizard, the Problems Found dialog box (Figure 3-3) appears listing all infected items.

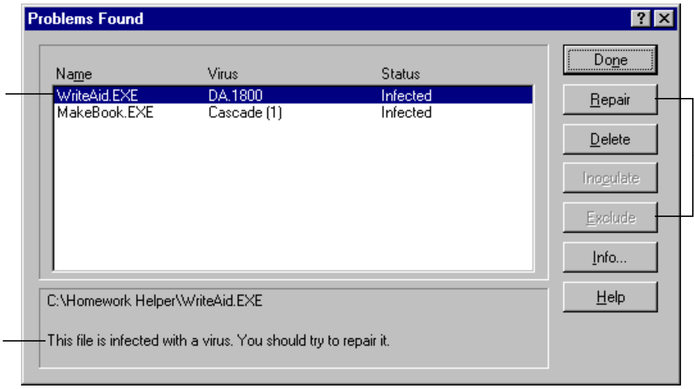
To resolve virus issues manually, item by item:

1. Select Manual in the Norton AntiVirus Repair Wizard (see Figure 3-1) and click Next.

   The Problems Found dialog box (Figure 3-3) appears listing each infected item.

2. Highlight an entry in the list box.
3. Read the message at the bottom of the dialog box to understand the type of problem that was found. It relates to the highlighted entry.
4. See “Command buttons,” on page 52 for information on the command buttons in the Problems Found dialog box, then click the appropriate button.

Figure 3-3 Problems Found dialog box



Name	Virus	Status
WriteAid.EXE	DA.1800	Infected
MakeBook.EXE	Cascade (1)	Infected

C:\Homework Helper\WriteAid.EXE

This file is infected with a virus. You should try to repair it.

Highlight an entry in the list box

Actions you can take to respond to the problem for the highlighted entry

Description of the problem for the highlighted entry

NOTE: Some users prefer to have a Virus Found alert generated immediately if a virus is detected during a scan, rather than waiting until the end of the scan. See "To set additional scanning options:," on page 79 if you want to configure for immediate notification.

Command buttons

The following table (below) explains all buttons that Norton AntiVirus may display to respond to virus issues. These buttons appear in the Problems Found dialog box, Auto-Protect virus alerts, and startup scan virus alerts. Later sections of this chapter give specific directions on how to respond to virus alerts. See "Eliminating viruses detected by Auto-Protect," on page 54 and "Eliminating viruses detected during startup scans," on page 62 for examples of virus alerts.

Note that some buttons may be dimmed or not displayed at all for the following reasons:

- The option is not permitted for your particular Norton AntiVirus configuration. These options are set on the Scanner, Auto-Protect, and Inoculation tabs. See Chapter 5, "Customizing Norton AntiVirus," on page 75, for information on setting options.
- Norton AntiVirus has determined that a particular action cannot be performed in the current situation.

Button	Result	Additional Information
Repair	Eliminates the virus and returns the infected file or boot record to its original state.	See “Responding to Auto-Protect virus found alerts,” on page 57.
	For inoculation changes, returns the file or boot record to its previous state.	See “Responding to Auto-Protect inoculation alerts,” on page 60.
Delete	Eliminates the virus by deleting the infected file.	Deleted files cannot be recovered. After the file is deleted, you must replace it with an uninfected copy.
Stop	Stops the current operation. If a scan is in progress, the scan stops. If you are accessing a file (such as launching a program or copying a file), access is denied.	Selecting Stop does not solve the problem reported. If it is a virus, the virus is prevented from activating, but remains on your computer and is still a source of risk.
Continue	Continues the current operation. If a scan is in progress, it continues. If you are accessing a file (such as launching a program or copying a file), access is granted.	Selecting Continue does not solve the problem that was reported to you. If Auto-Protect generated the alert, this may allow a virus to spread.
Exclude	Continues the operation and excludes the file from notifications of this kind in the future.	Use this command button only when you are sure it isn’t a real problem. Excluding a file means Norton AntiVirus won’t warn you again. See “Managing exclusions,” on page 83 for more information.
Inoculate	Stores data about the file or boot record that is used later to verify its integrity.	See “Inoculating files for the first time,” on page 60.
	Updates the inoculation data for a file or boot record that has changed since the last time it was inoculated.	Sometimes inoculation data changes can indicate the presence of an unknown virus. See “Reinoculating files that have changed,” on page 61.
Info...	Displays detailed information about the virus that was found.	See “Viewing the Virus List,” on page 72 for more information.

Eliminating viruses detected by Auto-Protect

Norton AntiVirus Auto-Protect, which constantly monitors for viruses, immediately displays a virus alert dialog box whenever an event concerning viruses occurs. These alerts are displayed in a character-based mode because all processing, including display processing, is stopped until the possible problem is resolved.

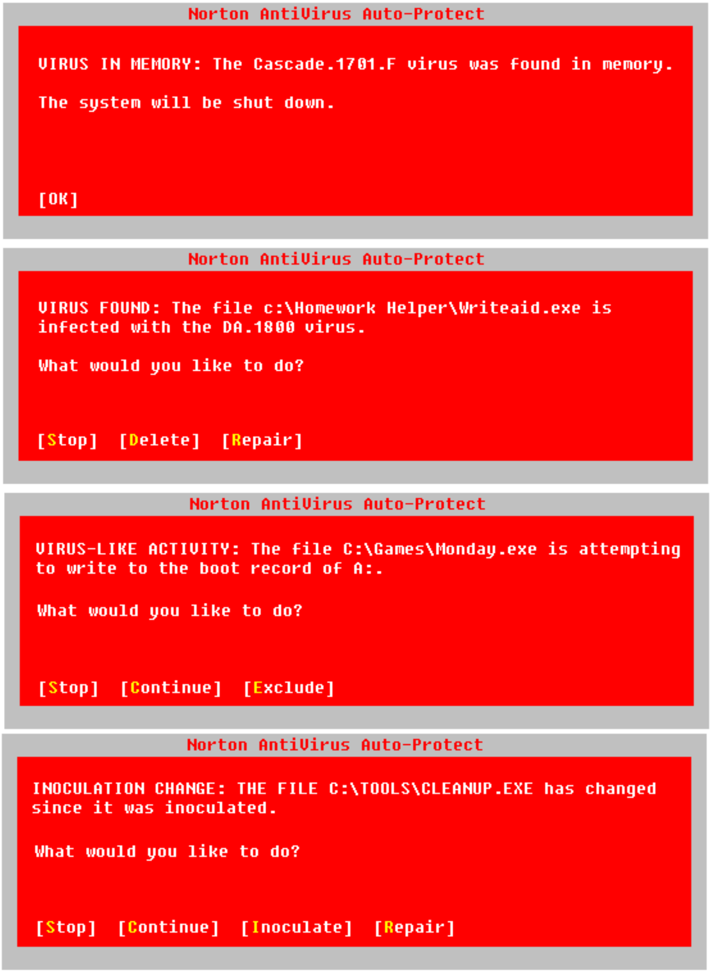
You are warned when:

- A virus is found in a program you are trying to run or a program file you are trying to copy.
- A virus is found in memory.
- A virus-like activity is detected (an operation that viruses often perform when spreading or damaging files).
- An inoculation issue is detected (either a file has not been inoculated or a file has changed since it was inoculated).

Figure 3-4 shows examples of the different types of Auto-Protect alerts.

NOTE: For a brief description of the command buttons in virus alerts, see “Command buttons,” on page 52.

Figure 3-4 Auto-Protect alerts



Virus in memory alert

```
Norton AntiVirus Auto-Protect

VIRUS IN MEMORY: The Cascade.1701.F virus was found in memory.

The system will be shut down.

[OK]
```

Virus found alert

```
Norton AntiVirus Auto-Protect

VIRUS FOUND: The file c:\Homework Helper\Writeaid.exe is
infected with the DA.1800 virus.

What would you like to do?

[Stop]  [Delete]  [Repair]
```

Virus-like activity alert

```
Norton AntiVirus Auto-Protect

VIRUS-LIKE ACTIVITY: The file C:\Games\Monday.exe is attempting
to write to the boot record of A:.

What would you like to do?

[Stop]  [Continue]  [Exclude]
```

Inoculation alert

```
Norton AntiVirus Auto-Protect

INOCULATION CHANGE: THE FILE C:\TOOLS\CLEANUP.EXE has changed
since it was inoculated.

What would you like to do?

[Stop]  [Continue]  [Inoculate]  [Repair]
```

If an Auto-Protect alert appears on your screen:

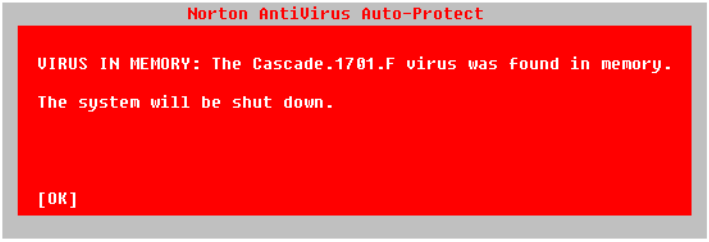
1. Read the message in the alert box to understand the type of problem that was found.
2. Refer to the appropriate section for instructions on how to proceed:
   - “Responding to Auto-Protect virus in memory alerts,” on page 56.
   - “Responding to Auto-Protect virus found alerts,” on page 57.
   - “Responding to Auto-Protect virus-like activity alerts,” on page 58.
   - “Responding to Auto-Protect inoculation alerts,” on page 60.

3 If you see a different message that you do not understand, see Appendix D, “System messages” on page 125 for more information.

Responding to Auto-Protect virus in memory alerts

A virus in memory means the virus has been activated, is spreading to other files, and in the worst case, is damaging files on your disk. When Norton AntiVirus detects a virus in memory, all processing stops immediately.

Figure 3-5 A virus in memory alert



```
Norton AntiVirus Auto-Protect

VIRUS IN MEMORY: The Cascade.1701.F virus was found in memory.

The system will be shut down.



[OK]
```

To respond to a virus in memory alert:

1 Press O for OK to shut down your computer.

2 Follow the Windows prompts to close applications and save data.

3 When the shutdown is complete, turn off your computer using the power switch.

Once you turn off your computer, the virus is removed from memory and is no longer spreading.

4 Use your write-protected Norton AntiVirus rescue disk set to restart your computer and scan again to find and remove the virus. See “Removing viruses from a shutdown computer,” on page 115 for more information.

If you don’t have a rescue disk set, you can use your write-protected Windows 95 Startup disk or a DOS 5.0 or higher system disk to reboot your computer. Then use your original installation Norton AntiVirus Disk 2 (Emergency) to run NAVDX. See “Removing viruses from a shutdown computer,” on page 115 for more information.

You can also create a bootable floppy disk on an uninfected computer that uses DOS 5.0 or higher. See your system manual for directions. Don’t use the infected computer; the virus could infect the boot disk you are trying to create. If you don’t have access to an uninfected computer, many dealers will create a bootable disk for you if you supply a blank floppy disk.

WARNING: If you don’t use your rescue disk or an uninfected, bootable floppy disk to restart your computer, you run the risk of activating the virus again.

Responding to Auto-Protect virus found alerts

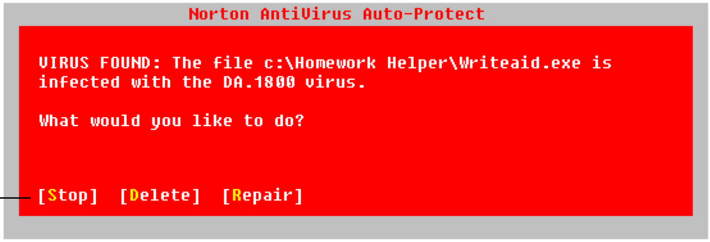
There are two ways to remove a virus from your computer:

- Repair the infected file, boot record, or master boot record.
- Delete the infected file from the disk.

  You cannot, however, delete infected system files, boot records, or master boot records because they contain information your computer uses to start up. See “What to do if repair is unsuccessful,” on page 63 for instructions on how to proceed if a repair cannot be made and the file cannot be deleted.

CAUTION: Files deleted by Norton AntiVirus cannot be recovered even with special file recovery utilities, such as the Norton Utilities.

Figure 3-6 A virus found alert



Norton AntiVirus Auto-Protect

VIRUS FOUND: The file c:\Homework Helper\Writeaid.exe is infected with the DA.1800 virus.

What would you like to do?

Actions you can take to respond to the alert

To repair an infected file or boot record:

1 Press R for Repair in the alert box.

  If the Repair button is not displayed, either Norton AntiVirus is configured not to enable it or the item cannot be repaired.

2 After repairing infected files or boot records, scan your drives and floppy disks with Norton AntiVirus to verify that there aren't any other files or boot records that contain viruses.

NOTE: Norton AntiVirus is preset to make backup copies of files before they are repaired. The backup files have a .VIR extension and appear in the folder listing with Virus Infected File as the file type. These backup files are not scanned in the future. Be sure to delete them once you know the repair was successful. For more information, see "Setting general scanning options," on page 90.

To delete an infected file:

1 Press D for Delete in the alert box, then follow the prompts on your screen.

  If the Delete button is not displayed, either Norton AntiVirus is configured not to enable it or the item cannot be deleted.

2 After deleting infected files, scan all of your drives and floppy disks with Norton AntiVirus to verify that there aren't any other files that contain viruses.

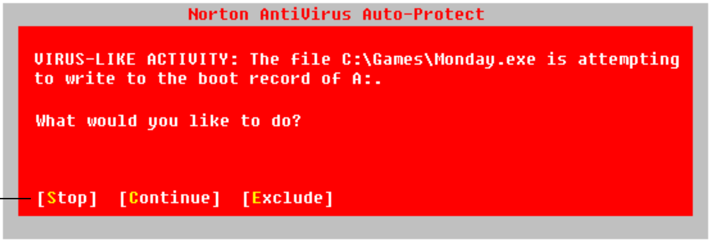
3 Once you are certain that your system is virus-free, replace the files you deleted with uninfected copies. Make sure you scan the replacement files before copying them to your hard disk.

TIP: If you forget which file needs replacing, look at the Activity Log for the name of the file. For information, see "Viewing the Activity Log," on page 40.

Responding to Auto-Protect virus-like activity alerts

A virus-like activity alert appears when Norton AntiVirus detects an activity that viruses often perform when spreading or doing damage to your files. These alerts are displayed in a character-based mode rather than in graphical mode. Norton AntiVirus stops all processing, including display processing, until the virus-like activity alert is resolved.

Figure 3-7 A virus-like activity alert



```
Norton AntiVirus Auto-Protect

VIRUS-LIKE ACTIVITY: The file C:\Games\Monday.exe is attempting
to write to the boot record of A:.

What would you like to do?


[Stop]  [Continue]  [Exclude]
```

Actions you can take to respond to the alert

NOTE: A virus-like activity alert does not necessarily mean your computer has a virus—it is simply a warning. It's up to you to decide whether the operation is valid in the context in which it occurred. For a description of each virus-like activity that Norton AntiVirus detects, see "Customizing automatic protection," on page 91.

To resolve an Auto-Protect virus-like activity alert:

Stop

If the activity detected is not related to what you are trying to do, press S for Stop to prevent the action from taking place.

For example, if you are playing a game and receive an alert stating that there is an attempt to write to the boot records of your hard disk, select Stop to prevent your disk from being modified.

Continue

If the message in the alert box describes an activity that is valid in the context of the application you are running, press C for Continue to allow the activity to proceed.

For example, if you are updating a software program and the alert warns you that there is an attempt to write to a program file, select Continue.

Exclude

If the activity is valid in the context of the application you are running and you don't want Norton AntiVirus to alert you of this activity (performed by this application) in the future, press E for Exclude.

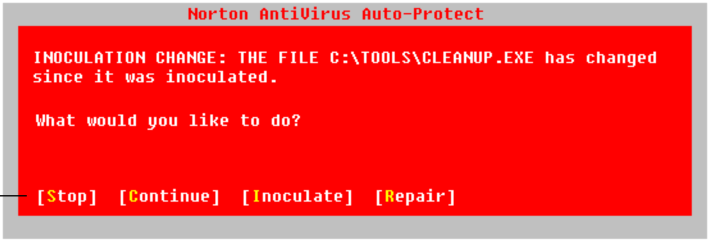
For example, if you are using a disk format utility to create a bootable floppy disk, you may want to select Exclude to prevent Norton AntiVirus from warning you every time you use the program to format a floppy disk.

Responding to Auto-Protect inoculation alerts

Norton AntiVirus displays inoculation alerts when:

- Files or boot records have not been inoculated.
- Files or boot records have changed since they were inoculated. Changes to inoculated files could indicate an unknown virus.

Figure 3-8 An inoculation alert



```
Norton AntiVirus Auto-Protect

INOCULATION CHANGE: THE FILE C:\TOOLS\CLEANUP.EXE has changed
since it was inoculated.

What would you like to do?

[Stop]  [Continue]  [Inoculate]  [Repair]
```

Actions you can take to respond to the alert

Inoculating files for the first time

Norton AntiVirus is preset to inoculate boot records and system files. If you choose to inoculate program files also, Norton AntiVirus is preset to scan uninoculated files it encounters for viruses and then inoculate them automatically.

If you choose Prompt, instead, for How To Respond When An Item Has Not Been Inoculated, Norton AntiVirus alerts you when an uninoculated file is encountered. You have the following options to resolve the inoculation alert. See "Customizing inoculation," on page 100 for directions to configure inoculation behavior.

To resolve an Auto-Protect new inoculation request:

Stop

Press S for Stop to halt the current operation.

For example, if you are trying to access a file (by launching a program), access is denied.

Continue

If you want to continue without taking any action, press C for Continue.

This response does not prevent Norton AntiVirus from notifying you about this file again in the future.

Inoculate

Press I for Inoculate to generate inoculation data for the file or boot record.

If you inoculate a file or boot record, Norton AntiVirus will notify you if the file ever changes. Changes in a file can sometimes indicate the presence of an unknown virus. Inoculation makes no change to the file or boot record itself, the inoculation data file is merely updated.

If you do not want to inoculate the file and you do not want future notifications about inoculating this file, press E for Exclude. Excluding the file means the file is at some risk of being infected by an unknown virus.

Reinoculating files that have changed

Inoculation changes in a file occur for these reasons:

- The file has changed for legitimate reasons since the last time you inoculated it. For example, you may have installed a new version of the software and not yet reinoculated the program file.
- The file contains a virus that is not in the definitions file (perhaps because you don’t have the most recent virus definitions or because it is a new virus for which Norton AntiVirus does not yet have a definition).

NOTE: Inoculation changes in boot records and system files may indicate the presence of an unknown virus. Boot records and system files change legitimately in very few situations, such as when you have installed a new operating system or repartitioned your hard disk.

To resolve an Auto-Protect inoculation change:

If you are certain the file or boot record has changed for legitimate reasons, press I for Inoculate to generate new inoculation information.

If you suspect a virus, press R for Repair to return the file or boot record to the way it was when you last inoculated it.

If you suspect a virus in a program file and have an uninfected backup copy of the file, press D for Delete; then replace it with the uninfected copy. Files deleted by Norton AntiVirus cannot be recovered.

If you do not want to reinoculate the file and you do not want future notifications about inoculating this file, press E for Exclude.

Eliminating viruses detected during startup scans

Norton AntiVirus startup scans catch viruses that infect the files and boot records your computer uses to ready itself for work. They are a vital part of virus protection because they make sure that your computer is virus-free each time you start it up. Viruses found during startup scans are a serious issue and must be resolved immediately: all files and data are at risk.

You are warned when:

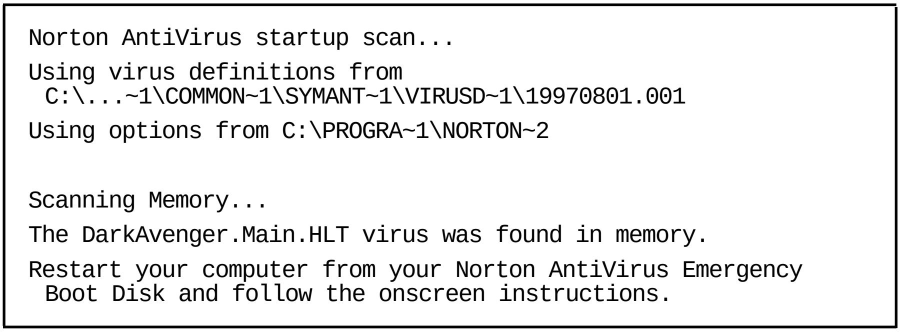
- A virus is found in memory.
- A virus is found in a system program or boot record.

Because startup scans are run before Windows loads, alerts are displayed as text messages on the screen. You are prompted to press a key to resolve the problem.

Responding to startup scan virus in memory alerts

A virus in memory means the virus has been activated, is spreading to other files, and in the worst cases, is damaging files on your disk. When Norton AntiVirus detects a virus in memory, all processing stops immediately.

Figure 3-9 A startup scan virus in memory alert



```
Norton AntiVirus startup scan...
Using virus definitions from
  C:\...~1\COMMON~1\SYMANT~1\VIRUSD~1\19970801.001
Using options from C:\PROGRA~1\NORTON~2


Scanning Memory...
The DarkAvenger.Main.HLT virus was found in memory.
Restart your computer from your Norton AntiVirus Emergency
  Boot Disk and follow the onscreen instructions.
```

To respond to a startup scan virus in memory alert:

1. Turn off your computer using the power switch.

   Once you turn off your computer, the virus is removed from memory and is no longer spreading.

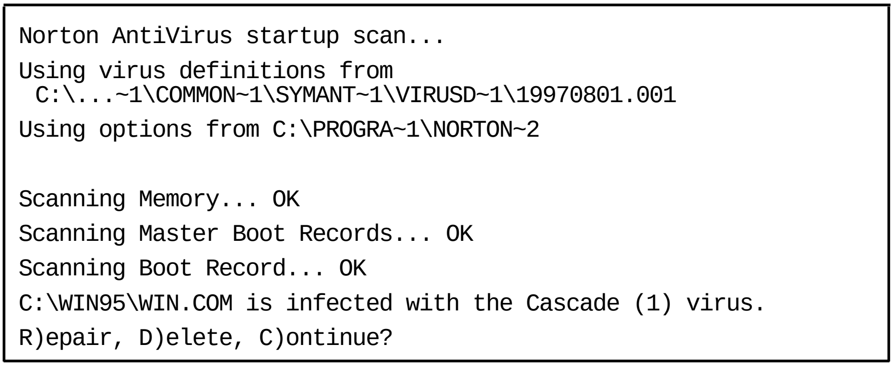
2. Use your write-protected Norton Rescue Boot Disk to restart your computer and scan again to find and remove the virus. See “Removing viruses from a shutdown computer,” on page 115 for more information.

If you don’t have a rescue disk set, you can use the Emergency Disk that was supplied with your original Norton AntiVirus package. See “Removing viruses from a shutdown computer,” on page 115 for more information.

Responding to startup scan virus found alerts

Virus found alerts on startup scans are a serious issue. A virus in a system file or boot record means your whole computer is at immediate risk. You should let Norton AntiVirus repair the infected item to eliminate the virus.

Figure 3-10 A startup scan virus found alert



```
Norton AntiVirus startup scan...
Using virus definitions from
 C:\...~1\COMMON~1\SYMANT~1\VIRUSD~1\19970801.001
Using options from C:\PROGRA~1\NORTON~2


Scanning Memory... OK
Scanning Master Boot Records... OK
Scanning Boot Record... OK
C:\WIN95\WIN.COM is infected with the Cascade (1) virus.
R)epair, D)elete, C)ontinue?
```

To repair a startup scan infected file or boot record:

1. Press R for Repair.
2. After repairing infected files or boot records, scan your drives and floppy disks again with Norton AntiVirus. This verifies that there aren’t any other files or boot records that contain viruses.

You cannot delete infected boot records, master boot records, and some system files to remove a virus because they contain information your computer uses to start up. See “What to do if repair is unsuccessful,” on page 63 for instructions on how to proceed if a repair cannot be made and the item cannot be deleted.

What to do if repair is unsuccessful

In the rare instance when Norton AntiVirus is not able to repair a file or boot record, you are notified that the repair was not successful.

Unable to repair a file

If Norton AntiVirus could not repair the infected file, the only way to remove the virus is to delete the file. After you let Norton AntiVirus delete the infected file, you can replace it with an uninfected copy. Use an uninfected backup copy or the original program disk that came with the application. If you don’t have a backup and can’t find the original disks, try contacting the program’s manufacturer for a replacement.

Unable to repair a system file

If the infected file is a system file, you cannot delete it. Restart your computer from an uninfected, write-protected floppy disk and reinstall Windows. You can use your Norton Rescue Boot Disk (see “Creating a rescue disk set,” on page 42) or the Windows 95 Startup Disk that you created when you installed Windows to start up. You could also use a boot disk from any version of DOS from version 5.0 or later.

Unable to repair a boot record

If Norton AntiVirus could not successfully repair the master boot record or a boot record on your hard disk, you can use your write-protected rescue disk to restore the boot record. See “Restoring your hard disk,” on page 116 for directions.

If Norton AntiVirus could not successfully repair a boot record on a floppy disk, you can still copy important files from the floppy disk to another disk. But be careful—the floppy disk is still infected. Scan any files you copy from the floppy disk for viruses again. After you’ve copied any important files from the infected floppy disk, either discard the disk or reformat it (use the Windows 95 “Full” option for Format type).

Removing viruses from compressed files

Although Norton AntiVirus will detect an infected file in a compressed file, it cannot repair the file in its compressed state.

To remove viruses from infected compressed files:

1. Create a temporary folder.
2. Click the Auto-Protect icon in the Windows taskbar to disable Auto-Protect temporarily.
3. Decompress the compressed file into the temporary folder.

4 Delete the infected compressed file.

5 Scan the temporary folder and repair or delete any infected files.

6 Recompress the files in the temporary folder, if desired.

7 Click the Auto-Protect icon in the Windows taskbar to enable Auto-Protect.

Keeping up with new viruses

4

Norton AntiVirus uses the information in its virus definitions files to detect viruses during scans. As new viruses are discovered, their virus definitions are added to the virus definitions files. To prevent newly discovered viruses from invading your computer, you should update your virus definitions files regularly. Updated virus definitions files are available monthly.

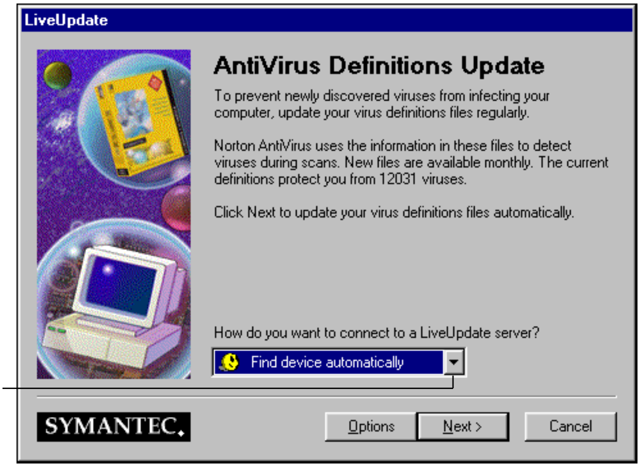
Automatically updating virus definitions

To ensure that you have current virus protection always, Norton AntiVirus can update the virus definitions files on your computer automatically. All that is required on your part is one of the following:

- An Internet connection
- A properly connected modem

Make it a practice to update your virus definitions once each month.

Figure 4-1 Update virus definitions automatically



LiveUpdate

AntiVirus Definitions Update

To prevent newly discovered viruses from infecting your computer, update your virus definitions files regularly.

Norton AntiVirus uses the information in these files to detect viruses during scans. New files are available monthly. The current definitions protect you from 12031 viruses.

Click Next to update your virus definitions files automatically.

How do you want to connect to a LiveUpdate server?

Find device automatically

Specify how to connect or let Norton AntiVirus choose automatically

To update virus definitions automatically:

1. In the Norton AntiVirus main window, click LiveUpdate (see Figure 4-1).
2. In the How Do You Want To Connect drop-down list box, select one of the following:
   - Find Device Automatically: Norton AntiVirus determines if you have an Internet connection or must connect using your modem.
   - FTP: Norton AntiVirus connects to the Symantec FTP (File Transfer Protocol) site on the Internet.
   - Modem: Norton AntiVirus dials a preset number and connects to a Symantec server through your modem.
3. Click Next to start the automatic update.

Whichever method you choose, Norton AntiVirus makes the connection, downloads the proper files, and installs them on your computer. You don’t have to do anything else.

When the update is finished, read the new Text Documents (*.TXT) in your Norton AntiVirus folder that are downloaded also. They contain late-breaking information about newly discovered viruses and any special precautions that you should take. C:\Program Files\Norton AntiVirus is the usual location for the Norton AntiVirus files.

NOTE: If the connection is made by modem, the long distance toll charge will appear on your telephone bill.

Using LiveUpdate Email

Whenever a major virus threat is discovered that requires an update to your virus protection, Symantec can notify you by email so you can run LiveUpdate immediately. The email includes an attachment that can start a LiveUpdate session for you.

To receive LiveUpdate Email:

1. Point your Internet browser to www.symantec.com/avcenter/newsletter.html
2. Fill out the registration form.

3. Click the Subscribe Me button.

   Symantec will notify you by email whenever protection updates are available.

To start a LiveUpdate session from the LiveUpdate Email:

- When you receive a LiveUpdate Email, launch or run the email attachment called LIVEUPDT.NLU from your mail program.

  You must launch or run the attachment; simply reading or viewing it will not work.

When the attachment runs, it automatically starts a LiveUpdate session on your computer. You don't have to do anything else.

Scheduling an automatic LiveUpdate

After you successfully complete a LiveUpdate to verify operation, you can schedule future LiveUpdates to run unattended at a predetermined frequency and time. For more information about using the Norton Program Scheduler, see "Scheduling virus scans," on page 43.

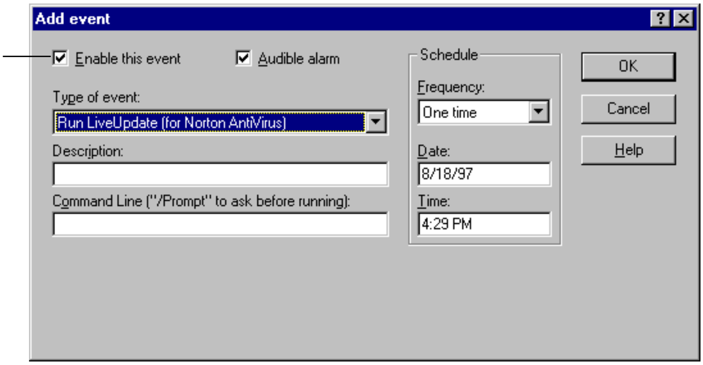
To schedule an automatic LiveUpdate:

1. Do one of the following to access the Norton Program Scheduler:
   - Click Scheduler in the Norton AntiVirus main window.
   - Choose NORTON PROGRAM SCHEDULER from the Windows Start menu.
2. Click Add.

   The Add Event dialog box appears.
3. Select Scheduled LiveUpdate in the Type Of Event drop-down list box.

   The dialog box changes to accept information specific to LiveUpdate.

Figure 4-2 Add event dialog box with Scheduled LiveUpdate selected



☑ Enable this event

☑ Audible alarm

Type of event: Run LiveUpdate (for Norton AntiVirus)

Description:

Command Line ("/Prompt" to ask before running):

Frequency: One time

Date: 8/18/97

Time: 4:29 PM

This must be checked for the LiveUpdate to run

4 Check Enable This Event.

If you uncheck this option, the LiveUpdate won't run.

5 Check Audible Alarm to hear a beep when LiveUpdate starts.

6 Type a brief description in the Description text box.

This text will appear in the events list in the Scheduler dialog box.

7 Type /PROMPT in the Command Line text box if you want to okay the LiveUpdate session when it is scheduled to run.

8 Select how often you want the LiveUpdate to occur in the Frequency drop-down list box.

9 Finish scheduling the LiveUpdate by entering the correct time, day, or date information, if necessary.

10 Click OK. If prompted for confirmation, also click OK in the confirmation dialog box.

Manually updating virus definitions

Symantec provides the latest virus definitions files with a program called Intelligent Updater, available for download at http://www.symantec.com and other sources listed in the Service and Support Solutions in this guide.

The name of the Intelligent Updater file, which changes with each update, uses the following form: mmddPbbL.EXE

mm	Month
dd	Day
P	Processor (I=Intel, A=Alpha)
bb	Platform (16=16-bit, 32=32-bit)
L	Language (A=US English)

For example, 1101I32A.EXE is the November 01, Intel, US English update for Windows NT or 95.

To install the new virus definitions:

1. Download the Intelligent Updater program to any folder on your computer.
2. From a My Computer or Windows Explorer window, double click the Intelligent Updater program.
3. Follow all prompts displayed by the update program.
4. The update program will install the new virus definitions files in the proper folder automatically.
5. Initiate a scan with Norton AntiVirus to activate the new virus definitions.
6. Restart your computer so that Auto-Protect uses the virus definitions files as well.
7. Read the new Text Documents (*.TXT) in your Norton AntiVirus folder for late-breaking information about newly discovered viruses and any special precautions that you should take.

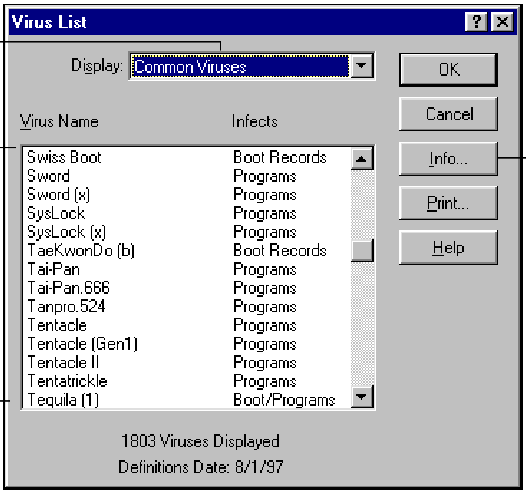
Viewing the Virus List

You can see which viruses Norton AntiVirus detects by viewing the list of virus names. These are the names of the viruses that can be identified from information in the virus definitions files. You can also view descriptions of particular viruses, including their symptoms and aliases.

To view the list of virus names:

- Click Virus List in the Norton AntiVirus main window.

Figure 4-3 Virus List



Display: Common Viruses

Virus Name	Infects
Swiss Boot	Boot Records
Sword	Programs
Sword (x)	Programs
SysLock	Programs
SysLock (x)	Programs
TaeKwonDo (b)	Boot Records
Tai-Pan	Programs
Tai-Pan.666	Programs
Tanpro.524	Programs
Tentacle	Programs
Tentacle (Gen1)	Programs
Tentacle II	Programs
Tentatrickle	Programs
Tequila (1)	Boot/Programs

1803 Viruses Displayed

Definitions Date: 8/1/97

Choose the category of viruses to display

Show details about the selected virus

The list of viruses for the category appears here

The list box displays the name of the virus and what it infects. You can view different categories of viruses by selecting a category from the Display drop-down list box.

All Viruses Displays all of the viruses that Norton AntiVirus can detect.

Common Viruses Displays the most common viruses. These are viruses that you are most likely to encounter.

Program Viruses Displays viruses that can infect program files that you run.

Boot Viruses Displays viruses that can infect boot records or master boot records on disks.

Stealth Viruses Displays viruses that try to conceal themselves from attempts to detect or remove them.

Polymorphic Viruses Displays viruses that appear differently in each infected file, making detection more difficult.

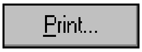
Multipartite Viruses Displays viruses that infect both program files and boot records.

Macro Viruses Displays viruses that infect Microsoft Word documents and Excel spreadsheets.

Windows Viruses Displays viruses that infect Windows programs.

Agent Viruses Displays viruses that infect agent programs (for example, programs that download software from the Internet.)

Click Info to view details about a particular virus, such as likelihood, characteristics, and aliases.



Click Print to print the virus list to a printer or to a file.

To search for a virus name:

1 Activate the virus list box by clicking inside the list box (see Figure 4-2).

2 Start typing the name of the virus you want to find.

A text box appears below the list box. As you type the consecutive letters in the virus name, the highlight moves to the corresponding virus name.

If the virus name you are looking for is not in the list, the list may not be displaying all viruses. To display all virus names, select All Viruses in the Display drop-down list box.

Customizing Norton AntiVirus

5

Norton AntiVirus is a powerful weapon in the war against computer viruses. The preset options from your Norton AntiVirus installation are designed to provide excellent protection for all computing environments. Unless you are a computer professional with special implementation requirements, it is unlikely that you will want or need to modify your Norton AntiVirus configuration. When you install Norton AntiVirus and accept the preset options, you are protected. You don’t have to change anything.

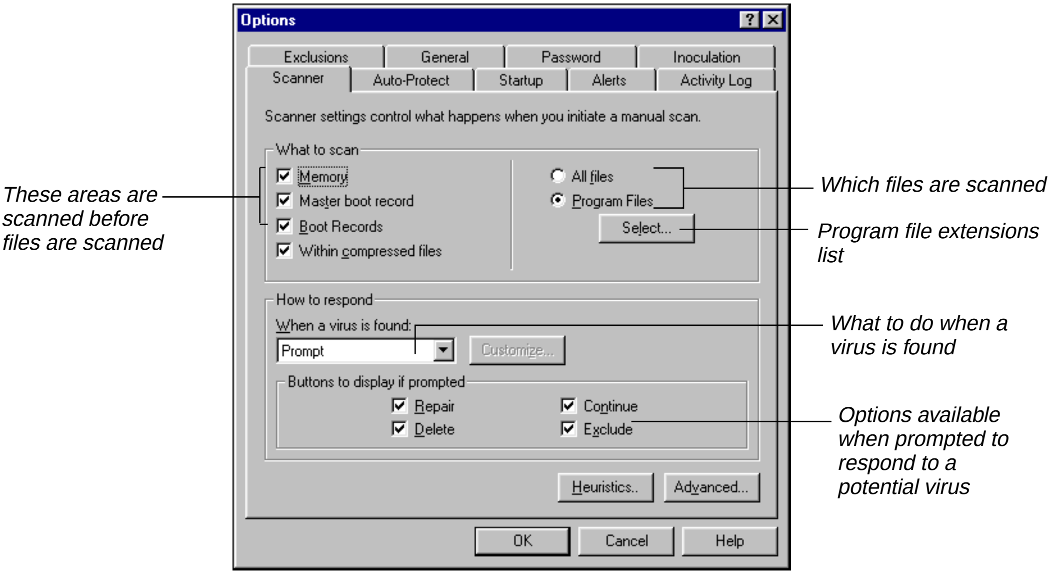
Customizing manual scan options

The manual scan options affect scans you initiate when you click the Scan Now button in the Norton AntiVirus main window or when scheduled scans occur.

To customize what to scan:

1. Click Options in the Norton AntiVirus main window.
2. Click the Scanner tab.

Figure 5-1 Scanner Settings



Options

Scanner settings control what happens when you initiate a manual scan.

What to scan

- ☑ Memory
- ☑ Master boot record
- ☑ Boot Records
- ☑ Within compressed files
- ○ All files
- ● Program Files

How to respond

When a virus is found: Prompt

Buttons to display if prompted

- ☑ Repair
- ☑ Delete
- ☑ Continue
- ☑ Exclude

These areas are scanned before files are scanned

Which files are scanned

Program file extensions list

What to do when a virus is found

Options available when prompted to respond to a potential virus

3 In the What To Scan group box, select which areas of your computer Norton AntiVirus should scan before it scans files. By default, these options are checked for general safety.

- Memory: Checks for viruses resident in your computer’s memory.

  It is important to check this option because viruses resident in memory are actively spreading to other files. If this option is left unchecked, a memory-resident virus can spread to every file scanned.

- Master Boot Record: Checks for viruses in the master boot record on your hard disk.
- Boot Records: Checks for viruses in the boot records on your hard disk and on any floppy disks you scan.
- Within Compressed Files: Norton AntiVirus scans files compressed using any one of several popular compression utilities (ZIP, LHA, and LZH). Compressed files within compressed files are not scanned. Scanning time may increase slightly if you have many compressed files.

4 Also specify in the What To Scan group box the types of files to scan:

- All Files: Scans all files in the specified folder or drive, including files less susceptible to viruses.
- Program Files: Scans files that are most likely to become infected. Only the files with an extension that is specified in the program file extensions list are scanned. For more information on which option to choose and on the program file extensions list, see "Selecting which files to scan," on page 80.

NOTE: The extensions for Microsoft Word documents and Microsoft Excel spreadsheets are included in the program files group. Although these are not program files, they can be infected by a new class of viruses called macro viruses.

5 Click OK to save your settings and close the dialog box, or continue with the next procedure.

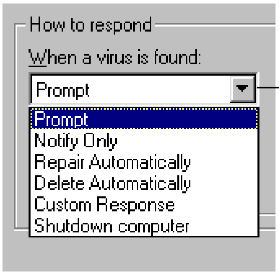
To customize how to respond when a virus is found:

1 Click Options in the Norton AntiVirus main window.

2 Click the Scanner tab (see Figure 5-2).

3 Select an option in the How To Respond drop-down list box.

Figure 5-2 What to do when a virus is found



Click to select an option

- Prompt: Informs you when a virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.
- Notify Only: Merely informs you when a virus is detected. You will not be able to repair or delete the infected file.

- Repair Automatically: Repairs an infected file or boot record without asking you. The results of the repair are displayed at the end of the scan and are also recorded in the Activity Log.

  Norton AntiVirus is preset to make backup copies of files before they are repaired. For more information, see "Setting general scanning options," on page 90.

- Delete Automatically: Deletes an infected file without asking you. The file deletion results are displayed at the end of the scan and are also recorded in the Activity Log. Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be recovered by any means.
- Custom Response: Lets you specify different actions for file, macro, and boot virus detections. After selecting Custom Response, click Customize to specify the actions.
- Shutdown Computer: Shuts down your computer when a virus is detected.

  To remove a virus after shutdown, insert your Norton Rescue Boot Disk (the first disk of your Norton AntiVirus rescue disk set) and restart your computer. Scan again to find and remove the virus. See "Removing viruses from a shutdown computer," on page 115 for directions.

CAUTION: Shutdown Computer instructs Norton AntiVirus to quit all applications and shut down immediately. You may not have an opportunity to save your work.

4 If you selected Prompt in step 3, specify in the Buttons To Display If Prompted group box which options you want Norton AntiVirus to make available when a virus is found:

- Repair: Allows you to repair the file or boot record. If the virus infects an item that cannot be repaired, such as an in-use file, the button will be dimmed.
- Delete: Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button will be dimmed.
- Continue: Allows you to continue scanning without resolving the problem. The Continue button applies only when Immediate Notification is turned on (see the next procedure for details on the Immediate Notification option).

- Exclude: Allows you to exclude the file from future checks for known viruses. Use caution when using this button; it can reduce your protection against viruses.

5 Click OK to save your settings and close the dialog box, or continue with the next procedure.

To set additional scanning options:

1 Click the Heuristics button in the Scanner tab (see Figure 5-2).

The Heuristic Scanning Options dialog appears (Figure 5-3).

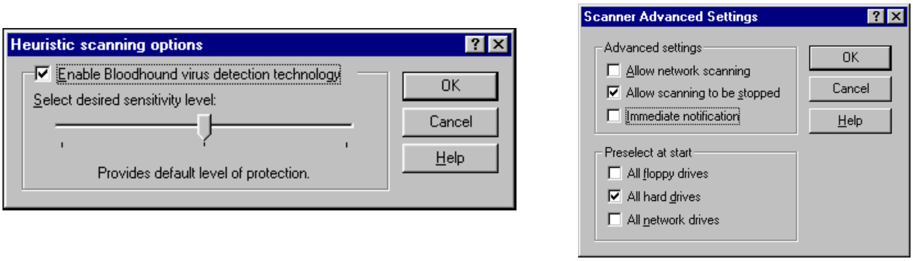
2 Make sure that Enable Bloodhound Virus Detection Technology is checked.

Norton AntiVirus includes a new technology called Bloodhound to dramatically increase your virus protection against difficult to detect viruses.

3 You can drag the pointer to increase Bloodhound processing in a high risk environment, but scanning will take a bit longer.

4 Click Ok to close the Heuristic Scanning Options dialog.

Figure 5-3 Additional Scanner settings



Heuristic scanning options

☑ Enable Bloodhound virus detection technology

Select desired sensitivity level:

Provides default level of protection.

Scanner Advanced Settings

Advanced settings

☐ Allow network scanning
☑ Allow scanning to be stopped
☐ Immediate notification

Preselect at start

☐ All floppy drives
☑ All hard drives
☐ All network drives

5 Click the Advanced button in the Scanner tab (see Figure 5-2).

The Scanner Advanced Settings dialog appears (see Figure 5-3).

6 Check the Advanced Settings options that you want to enable:

- Allow Network Scanning: Lets you scan network drives. See “Notes on scanning network drives,” on page 80 for network scanning restrictions.
- Allow Scanning To Be Stopped: Lets you halt a scan in progress. When this option is checked, the Stop button is available during a scan.

- Immediate Notification: Displays an alert box when a problem is detected while scanning. The alert box allows you to respond immediately, instead of waiting until the scan is completed.

NOTE: If you select Immediate Notification, the Repair Wizard does not appear at the end of the scan. All problems are resolved through the alert dialog boxes instead.

7 Specify in the Preselect At Start group box the drives that you want automatically selected in the Drives list box when you start Norton AntiVirus.

8 Click OK to save your settings and close the dialog box.

Notes on scanning network drives

Because you do not always have the same access privileges to a network drive as you have to a local drive, there are some restrictions when scanning network drives with Norton AntiVirus.

Drive access privileges	Operations you can perform
None	None
Read-Only	Scan, but not repair or delete infected files, or inoculate
Read-Write	Scan, repair, delete, and inoculate

Scanning network drives is more time consuming than scanning local drives. Other users may be creating, deleting, or moving files on a drive while Norton AntiVirus is scanning.

Selecting which files to scan

In most situations, scanning program files is adequate because viruses only infect and spread from these types of files. Following is an explanation of the file type options, so you can decide which setting is best for your situation.

All files

Scans every file—data files (such as databases, text files, and spreadsheets) and program files (such as system files, word processing programs, and utility programs). Scanning all files takes longer but includes any executable files or Microsoft Word documents that have non-standard file extensions. Scanning for program files only is usually sufficient—unless a virus is found on your computer. In this case, scan all files to ensure that every file on your disk is virus-free.

Program files only

Scans files with extensions contained in the program file extensions list. The list contains the most common extensions for executable files, which are most likely to become infected and spread viruses. Scanning only program files is sufficient in most cases.

NOTE: The extensions for Microsoft Word documents and Microsoft Excel spreadsheets are included in the program files group. Although these are not program files, they can be infected by a new class of viruses called macro viruses.

If you are using a specialized program that has an executable file extension not on the program file extensions list, you can add it to the list. Even if you don't add the extension to the list, Norton AntiVirus will probably catch the virus during a scan. A virus is most likely to infect one or more files that are on the program file extensions list before it infects a program with a non-standard file extension. After the virus is found, you can scan all files to ensure that every file on your disk is virus-free. See "Customizing manual scan options," on page 75 and "Customizing automatic protection," on page 91 for information on setting these options.

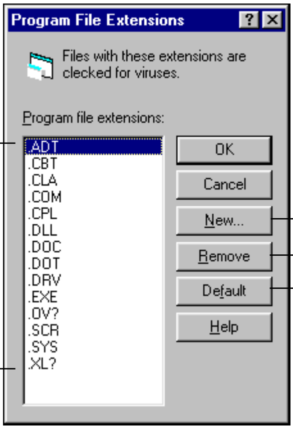
Specifying program file extensions

Norton AntiVirus uses the program file extensions list when scanning and inoculating program files. The list contains the file extensions for files most likely to become infected and spread viruses. File extensions are always three characters.

To view the current program file extensions:

1. Click Options in the Norton AntiVirus main window.
2. Click the Scanner tab.
3. Select the Program Files option in the What To Scan group box (see Figure 5-2).
4. Click Select.

Figure 5-4 Program File Extensions dialog box



Files with these extensions are checked for viruses.

Program file extensions:

.ADT
.CBT
.CLA
.COM
.CPL
.DLL
.DOC
.DOT
.DRV
.EXE
.OV?
.SCR
.SYS
.XL?

The current extensions are shown here

Add new extensions to the list

Remove extensions from the list

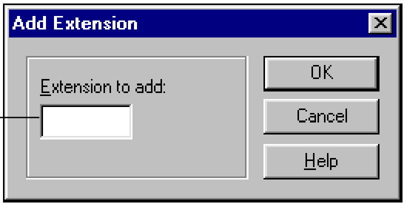
Return to original list

The file extensions list contains the majority of program file extensions. If you use custom applications that use unique file extensions, add them to the list.

To add a program file extension:

1 Click New in the Program File Extensions dialog box (Figure 5-5).

Figure 5-5 New Program File Extension dialog box



Type the new extension here

2 Type the new file extension in the Extension To Add text box and click OK.

You can use wildcards in the extension, but not to represent all three characters. For example, .OV? represents files with extensions that begin with .OV, such as .OVL and .OV1.

To remove a program file extension:

1 Select the file extension in the Program File Extensions dialog box (see Figure 5-5).

2 Click Remove and click OK.

To reset the list of program file extensions:

1 Click Default in the Program File Extensions dialog box (see Figure 5-5).

The list of extensions returns to the way it was when you installed Norton AntiVirus.

2 Click OK.

Managing exclusions

Norton AntiVirus refers to the entries in the exclusions list during all scans it performs. An exclusion is a condition or virus-like activity that would normally be detected, but you have told Norton AntiVirus not to check for a particular file. Excluding files doesn't mean "don't find viruses" (unless you specifically select that option); rather, it means "let some activity proceed" because you know a virus did not cause it.

CAUTION: Be careful. If you set an exclusion, a virus can creep in.

For example, because the operating system program FORMAT legitimately writes to the boot record of a floppy disk, you may want to exclude that activity for FORMAT.COM. By adding this activity to the exclusions list, you are telling Norton AntiVirus to ignore all writes to floppy disk boot records performed by FORMAT. But the file will still be checked for known viruses when scanned.

You set exclusions for items—drives, folders, groups of files, or single files. Each item can have more than one exclusion.

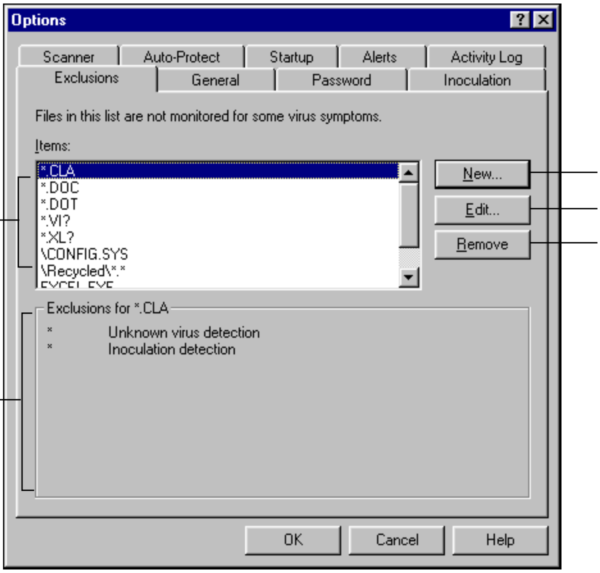
NOTE: An exclusion applies to a specific filename. If you move or rename a file, its exclusion doesn't move with it. You automatically invalidate the exclusion.

To view the exclusions list:

1 Click Options in the Norton AntiVirus main window.

2 Click the Exclusions tab.

Figure 5-6 Exclusions List Settings



Files in this list are not monitored for some virus symptoms.

Items:

```
*.CLA
*.DOC
*.DOT
*.VI?
*.XL?
\CONFIG.SYS
\Recycled\*.*
EXCEL.EXE
```

Exclusions for *.CLA

```
*        Unknown virus detection
*        Inoculation detection
```

Items not to check

The exclusions for the highlighted item are shown here

Add a new exclusion

Modify an existing exclusion

Delete an exclusion

3 Select a file or group of files in the Items list box.

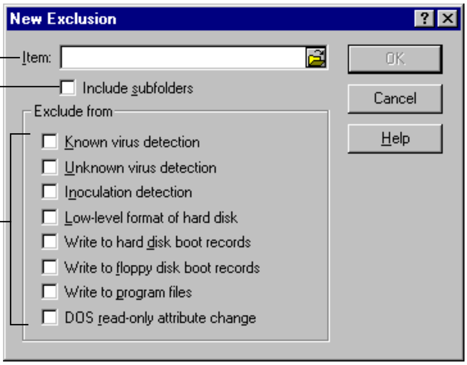
The activities excluded for the file or files are displayed in the Exclusions For group box.

NOTE: In most cases, items are added to the exclusions list when you click Exclude in an alert to resolve a virus detection event that you deem acceptable. Programmers, for example, may choose to turn off inoculation detection for files that are constantly changing during development. Although you can add exclusions to Norton AntiVirus manually, it is not a good idea unless you are sure of what you are doing.

To add exclusions manually:

1 Click New in the Exclusions tab (see Figure 5-7).

Figure 5-7 Adding a new exclusion



New Exclusion

Item:

☐ Include subfolders

Exclude from

☐ Known virus detection

☐ Unknown virus detection

☐ Inoculation detection

☐ Low-level format of hard disk

☐ Write to hard disk boot records

☐ Write to floppy disk boot records

☐ Write to program files

☐ DOS read-only attribute change

File or group of files to exclude

Also exclude files in subfolders if the item is a folder

Norton AntiVirus will not monitor the item for checked conditions

2 Type the pathname for the file or group of files in the Item text box.

3 Check Include Subfolders if you want to exclude files in descending folders also.

4 Check the activities that you want Norton AntiVirus to exclude from detection.

- Known Virus Detection: Exclude the item from checks for known viruses.
- Unknown Virus Detection: Exclude the item from checks for unknown viruses (Auto-Protect Virus Sensor).
- Inoculation Detection: Exclude the item from checks to see if it’s been inoculated and from checks for inoculation changes.
- Low-level Format Of Hard Disk: Exclude the item from checks for attempts to perform a low-level format of your hard disk, which obliterates all information on the disk.
- Write To Hard Disk Boot Records: Exclude the item from checks for attempts to write to the boot records on your hard disk. This action is performed legitimately by very few programs.
- Write To Floppy Disk Boot Records: Exclude the item from checks for attempts to write to the boot record on a floppy disk. This action is performed legitimately by very few programs.

- Write To Program Files: Exclude the item from checks for attempts to write to a program file. Some programs save configuration information within themselves rather than in a separate file.
- DOS Read-only Attribute Change: Exclude the item from checks for attempts to change a read-only file so that it can be written to. This option applies specifically to operations executed by DOS applications.

NOTE: Although excluding files from specific checks can be useful, be cautious when excluding files because it can also reduce your virus protection.

5. Click OK.

To modify an existing exclusion:

1. Select a file or group of files from the Items list box in the Exclusions tab (see Figure 5-7).
2. Click Edit and make the desired changes.
3. Click OK.

To remove an exclusion:

1. Select a file or group of files from the Items list box in the Exclusions tab (see Figure 5-7).
2. Click Remove and click OK.

   The exclusion is removed from the list so that complete virus protection is restored.

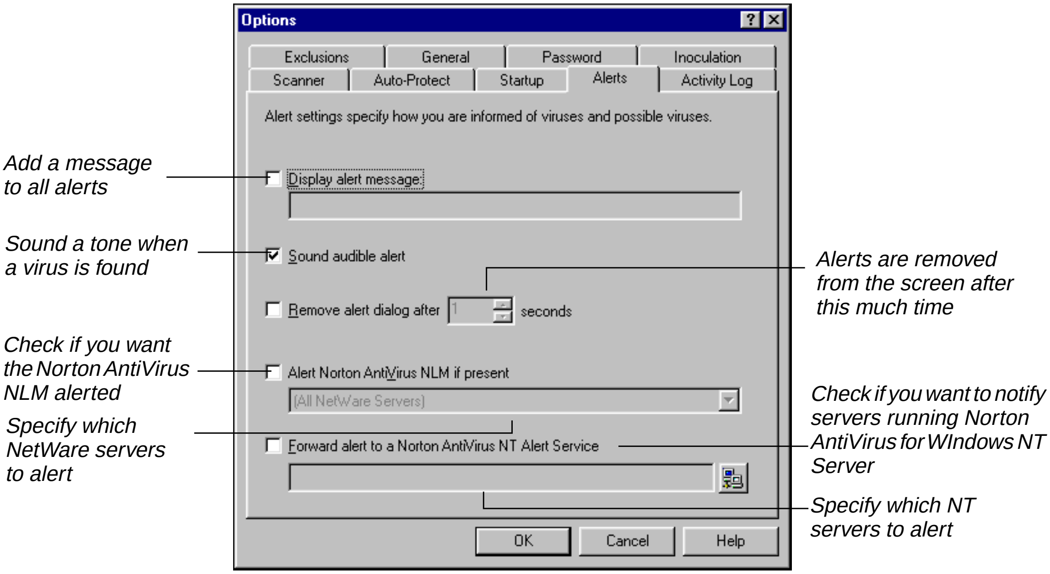
Customizing alerts

The alert settings define how Norton AntiVirus informs you that it has detected a virus or possible virus. These options apply to all scans that Norton AntiVirus performs (scans you initiate, scheduled scans, and scans performed automatically by Auto-Protect).

To customize alerts:

1. Click Options in the Norton AntiVirus main window.
2. Click the Alerts tab.

Figure 5-8 Alerts Settings



Alert settings specify how you are informed of viruses and possible viruses.

☐ Display alert message:

☑ Sound audible alert

☐ Remove alert dialog after 1 seconds

☐ Alert Norton AntiVirus NLM if present

(All NetWare Servers)

☐ Forward alert to a Norton AntiVirus NT Alert Service

Add a message to all alerts

Sound a tone when a virus is found

Check if you want the Norton AntiVirus NLM alerted

Specify which NetWare servers to alert

Alerts are removed from the screen after this much time

Check if you want to notify servers running Norton AntiVirus for WIndows NT Server

Specify which NT servers to alert

3 Check Display Alert Message to add a message with instructions or special warnings to all alerts that Norton AntiVirus displays. Then enter the message in the text box.

4 Check Sound Audible Alert if you want Norton AntiVirus to sound a tone when it alerts you of a virus.

5 Check Remove Alert Dialog After to specify how long notification dialog boxes stay on your screen. Then enter a number of seconds (between 1 and 99) in the Seconds text box.

6 Click OK.

Sending network alerts

When a virus or other Norton AntiVirus event is detected on a workstation, Norton AntiVirus can send alerts to the Norton AntiVirus for NetWare NLM over Novell NetWare networks. You can specify a particular server or notify all NetWare servers running the NLM. For networks with Windows NT servers, alerts can be forwarded to servers running Norton AntiVirus for Windows NT Server.

To set network alert options:

1. Click Options in the Norton AntiVirus main window.
2. Click the Alerts tab (see Figure 5-9).
3. For Novell NetWare networks, check the Alert Norton AntiVirus NLM If Present check box.
4. Do one of the following:
   - In the drop-down list box, select a specific NetWare server running the Norton AntiVirus NLM.
   - In the drop-down list box, select All NetWare Servers. Norton AntiVirus will alert all NetWare servers running the NLM.
5. For Windows NT servers, check Forward Alert To A Norton AntiVirus NT Alert Service.
6. Either type the name of the message relay target or click the browse button and select it from the network tree.
7. Click OK.

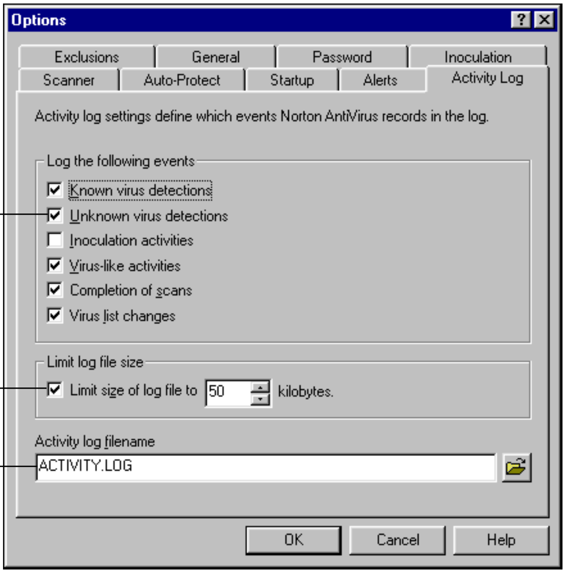
Customizing the Activity Log

The Activity Log contains a history of Norton AntiVirus activity. For example, Norton AntiVirus is preset to record detections of known viruses and the action performed on infected files (whether they were repaired, deleted, added to the exclusions list, or left untouched). You can customize the Activity Log to record other types of events (such as unknown virus detections and Virus List changes) as well.

To customize the Activity Log:

1. Click Options in the Norton AntiVirus main window.
2. Click the Activity Log tab.

Figure 5-9 Activity Log Settings



Activity log settings define which events Norton AntiVirus records in the log.

Log the following events

- ☑ Known virus detections
- ☑ Unknown virus detections
- ☐ Inoculation activities
- ☑ Virus-like activities
- ☑ Completion of scans
- ☑ Virus list changes

Limit log file size

☑ Limit size of log file to 50 kilobytes.

Activity log filename: ACTIVITY.LOG

Checked items are logged

Maximum size for the Activity Log file

Activity Log file

3 In the Log Following Events group box, check each type of event that you want Norton AntiVirus to record:

- Known Virus Detections: Records detections of known viruses (Auto-Protect Virus Sensor).
- Unknown Virus Detections: Records detections of unknown viruses (viruses not yet identified in the Virus List).
- Inoculation Activities: Records detections of uninoculated files and changes in a file’s inoculation data.
- Virus-like Activities: Records detections of virus-like activities (activities that many viruses perform when spreading or damaging data, such as an attempt to format your hard disk).
- Completion Of Scans: Records the date and ending time of scans that you initiate and scheduled scans.
- Virus List Changes: Records changes to the Virus List.

4 If you want to limit the size of the Activity Log file, check Limit Size Of Log File To, then enter the desired size in the Kilobytes text box.

When the Activity Log reaches the specified size, each new entry added to the activity log causes the oldest entry or entries to be deleted.

5 Enter the pathname for the Activity Log file in the Activity Log Filename text box.

6 Click OK to save settings and close the dialog box.

Setting general scanning options

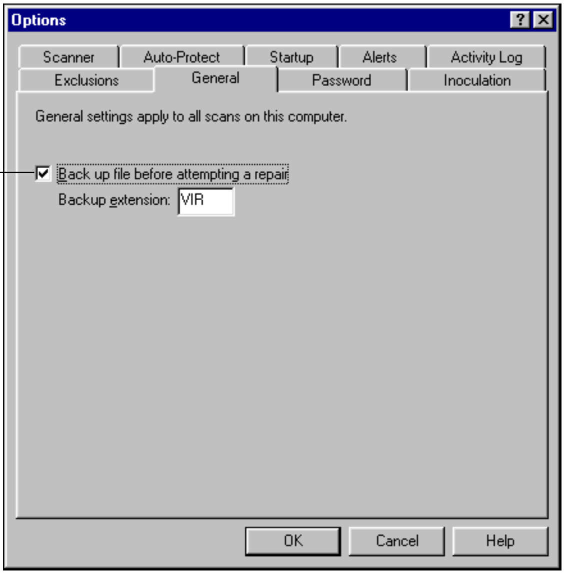
The general scanning options apply to all scans—scans you initiate, scheduled scans, and scans performed by Auto-Protect.

To customize general scanning options:

1 Click Options in the Norton AntiVirus main window.

2 Click the General tab.

Figure 5-10 General Settings



General settings apply to all scans on this computer.

☑ Back up file before attempting a repair

Backup extension: VIR

Makes a backup copy of the virus-infected file

3 Check Back Up File Before Attempting A Repair to have Norton AntiVirus make a copy of the infected file before repairing it. The default extension is .VIR for virus-infected, backed-up files. You can, however, enter a different extension for the backup file in the Backup Extension text box.

All files with the backup extension are added automatically to the exclusions list so they will not be reported again during a scan. The file type appears as Virus Infected File when you list files using the Windows Explorer.

NOTE: Delete these backup files after you determine that the repair operation is successful. Even though the infected backup files can't be run (because of the .VIR file extension), they contain viruses.

4 Click OK.

Customizing automatic protection

The automatic protection feature protects your computer against viruses by:

- Checking programs for viruses when you run them and floppy disks for viruses when you access them.
- Monitoring your computer for signs of unknown viruses or virus-like activities.
- Preventing viruses from getting onto your computer when you copy or install files on your system.

For information on other options that affect Auto-Protect scans, see "Customizing manual scan options," on page 75.

Auto-Protecting program files

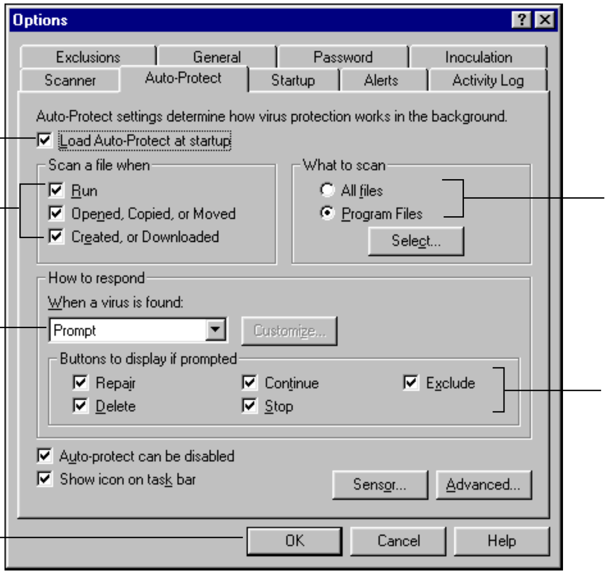
Norton AntiVirus can check for viruses whenever you open a file or run a program.

To Auto-Protect program files:

1 Click Options in the Norton AntiVirus main window.

2 Click the Auto-Protect tab.

Figure 5-11 Auto-Protect Settings



Options

Auto-Protect settings determine how virus protection works in the background.

☑ Load Auto-Protect at startup

Scan a file when

☑ Run
☑ Opened, Copied, or Moved
☑ Created, or Downloaded

What to scan

○ All files
● Program Files

How to respond

When a virus is found: Prompt

Buttons to display if prompted

☑ Repair ☑ Continue ☑ Exclude
☑ Delete ☑ Stop

☑ Auto-protect can be disabled
☑ Show icon on task bar

Check to make sure Auto-Protect is always loaded

Files are scanned when accessed in these ways

What to do when a known virus is found

Click OK to save settings and exit the dialog box

Which files are scanned

Options available when prompted to respond to a known virus

3 Check Load Auto-Protect At Startup to make sure automatic protection is on every time you start your computer.

NOTE: Unchecking this option significantly reduces protection against viruses.

4 Specify in the Scan A File When group box when Norton AntiVirus should scan the files you use:

- Run: Scans a program file each time you run it.
- Opened: Scans files when they are opened. For example, when you copy a file, Norton AntiVirus scans the file you are copying.
- Created: Scans files when they are created on your drive by an installation program, by decompressing files, or by downloading files from a bulletin board system.

5 Select an option in the What To Scan group box:

- All files: Scans all files that you access, includes files less likely to contain viruses.
- Program Files: Scans files that are most likely to become infected. Only the files with an extension that is specified in the program file extensions list are scanned.

For more information on which option to choose and on the program file extensions list, see “Selecting which files to scan,” on page 80.

6 Click OK to save your settings and close the dialog box, or continue to the next procedure.

To customize how to respond when a virus is found:

1 Click Options in the Norton AntiVirus main window.

2 Click the Auto-Protect tab (see Figure 5-12).

3 Select an option for how to respond in the When A Virus Is Found drop-down list box:

- Prompt: Informs you when a known virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.
- Deny Access: Prevents you from using a file when a known virus is detected. These events are recorded in the Activity Log.
- Repair Automatically: Repairs an infected file or boot record without notifying you. The results of the repair are recorded in the Activity Log.

  Norton AntiVirus is preset to make backup copies of files before they are repaired. For more information, see “Setting general scanning options,” on page 90.
- Delete Automatically: Deletes an infected file without asking you. The file deletion results are recorded in the Activity Log. Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be recovered.
- Custom Response: Lets you specify different actions for file, macro, and boot virus detections. After selecting Custom Response, click Customize to specify the actions.
- Shutdown Computer: Shuts down your computer when a known virus is detected. You must use your Norton AntiVirus rescue disk set to both reboot your computer and scan again to find and remove the virus from the infected file or boot record.

CAUTION: Shutdown Computer instructs Norton AntiVirus to quit all applications and shut down immediately. You may not have an opportunity to save your work, but it will stop a virus from spreading.

4. If you selected Prompt in step 3, specify in the Buttons To Display If Prompted group box which options to make available when a known virus is found:
   - Repair: Allows you to repair the file or boot record.
   - Delete: Allows you to delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is not displayed.
   - Continue: Allows you to continue accessing the file. If you select the Continue button, you may activate the virus.
   - Stop: Allows you to stop the file access. The virus will not be activated, but the file is still infected.
   - Exclude: Allows you to exclude the file from future checks for known viruses. Use caution when using this button; it reduces your protection against viruses.
5. Check Auto-Protect Can Be Disabled if you want to be able to temporarily turn automatic protection off by clicking the Auto-Protect icon on the Windows taskbar.
6. Check Show Icon On Taskbar to remind you that automatic protection is in force and to permit the temporary enabling or disabling of Auto-Protect.
7. Click OK to save your settings and close the dialog box or continue to the next procedure.

Protecting against unknown viruses with Virus Sensor

An unknown virus is one that has not yet been identified. Because there is no definition for the virus, it will not be detected by a scan for known viruses. Auto-Protect, however, catches unknown viruses by using a special Virus Sensor technology to monitor computer activity for the signs of a virus trying to replicate.

The Virus Sensor is an extra layer of protection that is not turned on automatically during Norton AntiVirus installation. If you choose to turn it on, you will receive alerts during the course of regular operation that may or may not be caused by a virus. You will have to judge if the activity was legitimate in the context of your operation or a virus activity on an event by event basis.

You can also protect against unknown viruses by inoculating files. See “Customizing inoculation,” on page 100.

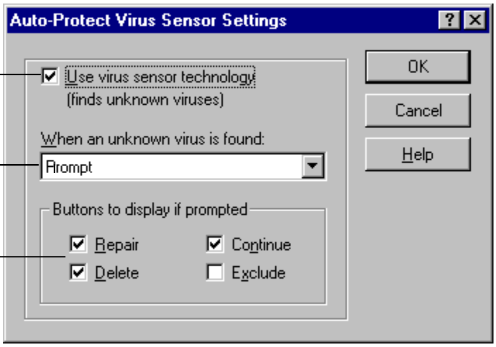
To monitor for unknown viruses:

1 Click Options in the Norton AntiVirus main window.

2 Click the Auto-Protect tab.

3 Click Sensor in the Auto-Protect tab (Figure 5-12).

Figure 5-12 Virus Sensor Settings



Auto-Protect Virus Sensor Settings

☑ Use virus sensor technology (finds unknown viruses)

When an unknown virus is found: Prompt

Buttons to display if prompted

☑ Repair ☑ Continue

☑ Delete □ Exclude

Check to have Norton AntiVirus monitor for unknown viruses

What to do when an unknown virus is found

Options available when prompted to respond to an unknown virus

4 Check Use Virus Sensor Technology to detect when your programs become infected by an unknown virus.

5 Select an option in the When An Unknown Virus Is Found drop-down list box:

- Prompt: Informs you when an unknown virus is found and allows you to choose how to respond. Select Prompt to have the most control over what happens to an infected file.
- Repair Automatically: Repairs an infected file without asking you. The outcome of the repair is recorded in the Activity Log.

  Norton AntiVirus is preset to make backup copies of files before they are repaired. For more information, see "Setting general scanning options," on page 90.
- Delete Automatically: Deletes an infected file without asking you. The deletion is recorded in the Activity Log. Be careful if selecting this option. Files deleted by Norton AntiVirus cannot be recovered.
- Shutdown Computer: Shuts down your computer when an unknown virus is detected.

6 If you selected Prompt in step 5, specify in the Buttons To Display If Prompted group box which options to make available when an unknown virus is found:

- Repair: Allows you to repair the file.
- Delete: Allows you to delete the file.
- Continue: Allows you to continue without taking action on the file. The file remains infected with the unknown virus.
- Exclude: Allows you to exclude the file from future checks for unknown viruses. Using this button can reduce your protection against unknown viruses.

7 Click OK to close the dialog box.

8 Click OK to save your settings and close the Options dialog box, or continue to the next procedure.

Monitoring for virus-like activities

A virus-like activity is an action that viruses typically perform when damaging your files or spreading through your system. Although some applications perform these actions for valid reasons, Norton AntiVirus can monitor for the activities to prevent them from being performed by an unknown virus.

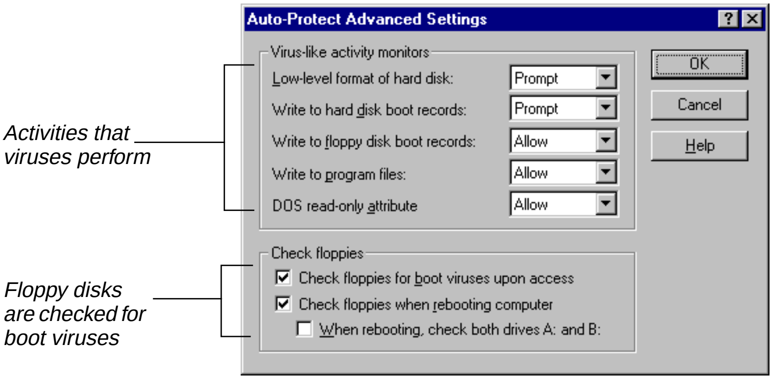
To monitor for virus-like activities:

1 Click Options in the Norton AntiVirus main window.

2 Click the Auto-Protect tab.

3 Click Advanced in the Auto-Protect tab (see Figure 5-12).

Figure 5-13 Auto-Protect Advanced Settings



Auto-Protect Advanced Settings

Virus-like activity monitors

Low-level format of hard disk: Prompt

Write to hard disk boot records: Prompt

Write to floppy disk boot records: Allow

Write to program files: Allow

DOS read-only attribute: Allow

Check floppies

☑ Check floppies for boot viruses upon access

☑ Check floppies when rebooting computer

□ When rebooting, check both drives A: and B:

Activities that viruses perform

Floppy disks are checked for boot viruses

4 Select a monitoring option in each drop-down list box to specify what Norton AntiVirus should do when it detects the virus-like activity:

- Allow: Allows the activity to continue every time without informing you. Selecting Allow offers you no protection against an unknown virus performing the activity.
- Prompt: Informs you when a program tries to perform the activity and allows you to decide whether to Continue, Stop, or Exclude. Although excluding files from specific checks can be useful, be careful. Excluding files can reduce your virus protection.
- Don't Allow: Prevents the activity from occurring every time it is detected.

The virus-like activities include:

- Low-level Format Of Hard Disk: All information on the disk is erased and cannot be recovered. This type of format is generally performed by the manufacturer. If this activity is detected, it almost certainly indicates an unknown virus at work.
- Write To Hard Disk Boot Records: Very few programs write to hard disk boot records. Unless you are specifically using a program that writes to the hard disk boot records, such as FORMAT, this activity probably indicates a virus.
- Write To Floppy Disk Boot Records: Only a few programs (such as the operating system FORMAT or SYS commands) write to floppy disk boot records.
- Write To Program Files: Some programs save configuration information within themselves. Although this activity often happens legitimately, it could indicate an unknown virus at work.
- DOS Read-Only Attribute Change: Many programs change a file's read-only attribute. Although this activity often happens legitimately, it could indicate an unknown virus at work. This option applies specifically to operations executed by DOS applications.

5 Click OK to close the dialog box.

6 Click OK to save your settings and close the Options dialog box, or continue to the next procedure.

Auto-Protecting floppy disks

Because boot viruses are most likely to spread through floppy disks, it is important to check each floppy disk you use. Norton AntiVirus can monitor floppy disks when you work with them or if you accidentally leave one in your disk drive while shutting down your computer.

To Auto-Protect floppy disks:

1. Click Options in the Norton AntiVirus main window.
2. Click the Auto-Protect tab.
3. Click Advanced in the Auto-Protect tab.
4. In the Check Floppies group box (see Figure 5-14), specify how you want Norton AntiVirus to check for boot viruses on floppy disks:
   - Check Floppies For Boot Viruses Upon Access: Checks for boot viruses on each floppy disk you access (such as, when you list the folder, copy a file, write to a file, or run a file).
   - Check Floppies When Rebooting Computer: Checks a floppy disk in drive A: for boot viruses when you shut down your computer.
   - When Rebooting, Check Both Drives A: and B: Also checks a floppy disk in drive B: for boot viruses when you shut down your computer. Select this option if you have a system that can boot from a disk in the B: drive.
5. Click OK to close the dialog box.
6. Click OK to save your settings and close the dialog box.

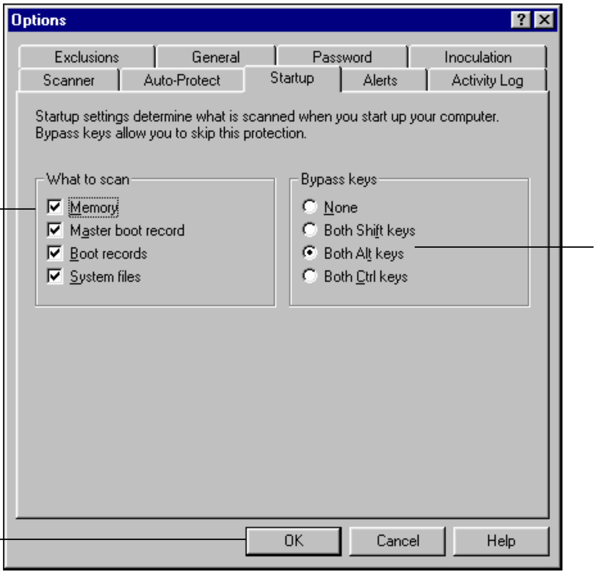
Customizing startup protection

Checking for viruses during system startup is an important step in preventing viruses from activating or spreading. If a system file is infected, the virus will activate when you start up your computer and may infect other programs you run during the day.

To customize system startup protection:

1. Click Options in the Norton AntiVirus main window.
2. Click the Startup tab.

Figure 5-14 Startup Settings



Startup settings determine what is scanned when you start up your computer. Bypass keys allow you to skip this protection.

What to scan

- ☑ Memory
- ☑ Master boot record
- ☑ Boot records
- ☑ System files

Bypass keys

- ○ None
- ○ Both Shift keys
- ● Both Alt keys
- ○ Both Ctrl keys

Norton AntiVirus scans these areas when you start your computer

Key combination to skip the startup scan

Click OK to save settings and exit the dialog box

3 Specify in the What To Scan group box the areas that you want Norton AntiVirus to scan each time you start your computer:

- Memory: Scans for viruses resident in your computer’s memory. Viruses in memory can spread to other files you access.
- Master Boot Record: Scans for boot viruses in the master boot record.
- Boot Records: Scans for boot viruses in the boot records on your hard disk.
- System Files: Scans the operating system files your computer uses to startup and run Windows.

4 Specify in the Bypass Keys group box the keystroke combination you want to use to prevent automatic protection from loading when your computer starts up. The bypass key may be useful if you are trying to resolve a system startup problem or configuration conflict.

Select None if you don’t want a bypass key combination.

5 Click OK.

Customizing inoculation

Inoculating files offers an extra level of protection against unknown viruses. When you inoculate a program file, system file, or boot record, Norton AntiVirus records critical information about it (similar to taking a fingerprint). Subsequently, Norton AntiVirus monitors the inoculated item for changes that could indicate an unknown virus.

Customizing inoculation involves specifying what gets inoculated during a scan and how to respond when a change has occurred or when an uninoculated file is encountered.

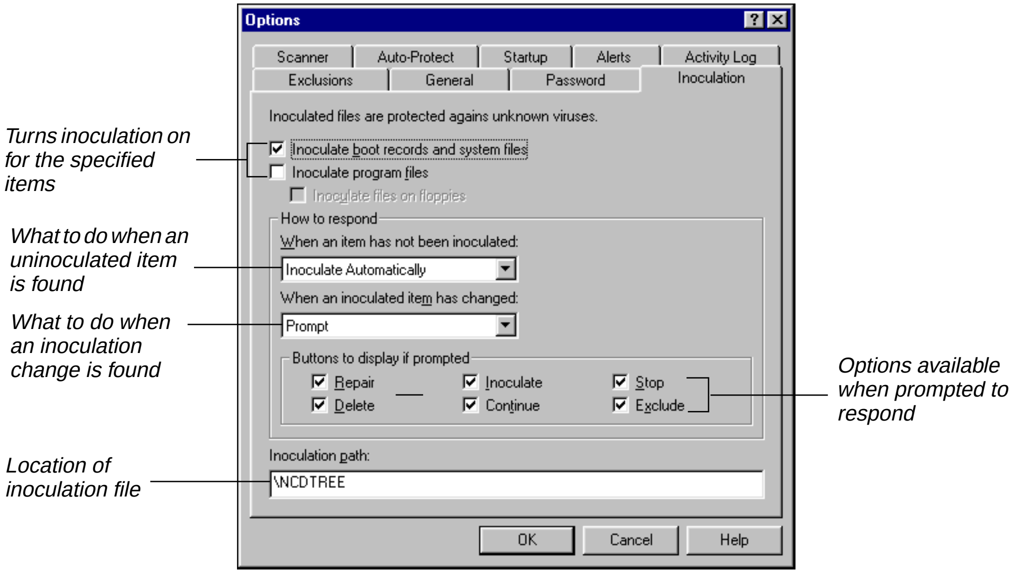
Inoculation of program files is an extra layer of protection that is not turned on automatically during Norton AntiVirus installation. If you choose to turn it on, you will receive alerts during the course of regular operation that may or may not be caused by a virus. You will have to judge if the activity was legitimate in the context of your operation or a virus activity on an event by event basis.

To customize what to inoculate:

1 Click Options in the Norton AntiVirus main window.

2 Click the Inoculation tab.

Figure 5-15 Inoculation Settings



Options

Inoculated files are protected agains unknown viruses.

☑ Inoculate boot records and system files
□ Inoculate program files
□ Inoculate files on floppies

How to respond

When an item has not been inoculated: Inoculate Automatically

When an inoculated item has changed: Prompt

Buttons to display if prompted

☑ Repair ☑ Inoculate ☑ Stop
☑ Delete ☑ Continue ☑ Exclude

Inoculation path: \NCDTREE

Turns inoculation on for the specified items

What to do when an uninoculated item is found

What to do when an inoculation change is found

Location of inoculation file

Options available when prompted to respond

3 Check Inoculate Boot Records And System Files so that the master boot record, boot records, and system files on your hard disk receive inoculation protection.

TIP: Be sure to check Inoculate Boot Records And System Files so that Norton AntiVirus can detect unknown viruses in boot records.

4 Check Inoculate Program Files to check files for inoculation on the hard disks and network drives you use. Check Inoculate Files On Floppies if you also want to inoculate files on the floppy disks you use.

5 Click OK to save changes and close the dialog box, or continue with the next procedure.

To customize how to respond to inoculation issues:

1 Click Options in the Norton AntiVirus main window.

2 Click the Inoculation tab (see Figure 5-15).

3 Select an option in the When An Item Has Not Been Inoculated drop-down list box.

- Prompt: Informs you when a file or boot record has not been inoculated and allows you to choose how to respond.
- Inoculate Automatically: Inoculates each uninoculated file or boot record as soon as it is detected. The item is scanned for known viruses before it is inoculated to ensure it is virus-free.
- Notify Only – Don’t Inoculate: Merely informs you that a file or boot record is uninoculated. It does not inoculate the item.
- Deny Access: Informs you that a program file has not been inoculated and does not allow you to use the program. (This option does not apply to uninoculated boot records or system files.)

4 Select an option in the When An Inoculated Item Has Changed drop-down list box:

- Prompt: Informs you when a file or boot record has changed and allows you to choose how to respond.
- Notify Only - Don’t Reinoculate: Merely informs you that the file or boot record has changed. It does not reinoculate the item.
- Deny Access: Informs you when an inoculation change is detected and prevents you from using the file. (This option does not apply to boot records.)

5 If you selected Prompt in step 3 or 4, specify in the Buttons To Display If Prompted group box which options you want available when an inoculation issue is found:

- Repair: Allows you to repair a file or boot record with an inoculation change, returning the item to its state when it was last inoculated.

  Norton AntiVirus is preset to make backup copies of files before they are repaired. For more information, see “Setting general scanning options,” on page 90.

- Delete: Allows you to delete a program file with an inoculation change. For boot records and system files, the button is not displayed.
- Inoculate: Allows you to inoculate a file or boot record or reinoculate a changed file or boot record.
- Continue: Allows you to continue the current operation (scanning or accessing a file). No change is made to the inoculation data.
- Stop: Allows you to stop the current operation (scanning or accessing a file). No change is made to the inoculation data.
- Exclude: Allows you to exclude the file from future checks for inoculation and inoculation changes.

6 Type a folder path for the inoculation files in the Inoculation Path text box. The default path is \NCDTREE for the inoculation files.

When you inoculate files and boot records, an inoculation file is placed in the specified location on each drive you inoculate.

NOTE: If you are inoculating files on network drives, you must have write access to this folder on the network drive. You do not need write access to the files you inoculate.

7 Click OK to save your settings and close the dialog box.

Setting password protection

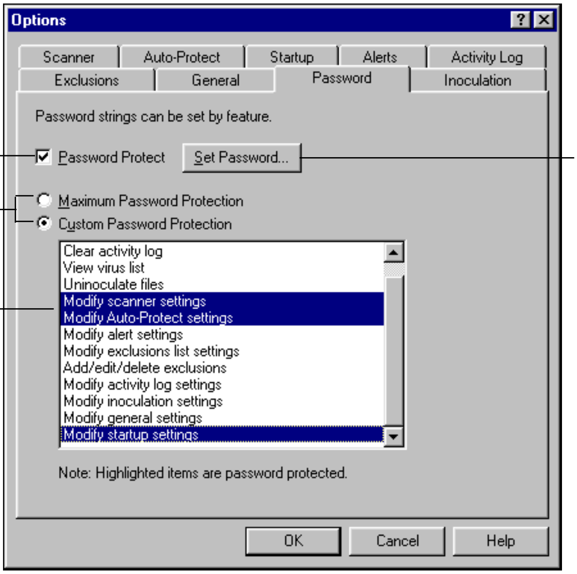
Password protection guarantees that your Norton AntiVirus configuration will not be modified. You can protect selected features or all configurable options.

To password-protect features:

1 Click Options in the Norton AntiVirus main window.

2 Click the Password tab.

Figure 5-16 Password Settings



Password strings can be set by feature.

☑ Password Protect [Set Password...]

○ Maximum Password Protection
● Custom Password Protection

- Clear activity log
- View virus list
- Uninoculate files
- Modify scanner settings (highlighted)
- Modify Auto-Protect settings (highlighted)
- Modify alert settings
- Modify exclusions list settings
- Add/edit/delete exclusions
- Modify activity log settings
- Modify inoculation settings
- Modify general settings
- Modify startup settings (highlighted)

Note: Highlighted items are password protected.

Turn on password protection

Protect all features or only selected ones

Click to select or deselect a feature for protection

Specify the password

3 Check Password Protect to turn on the password protection feature.

4 Do one of the following:

- To protect all Norton AntiVirus features, select Maximum Password Protection.
- To protect only specified features, select Custom Password Protection; then click the features you want to protect in the list box.

5 Click Set Password and enter the password you want to use in the Set Password dialog box. The same password applies to all protected options.

Passwords can be from 1 to 16 characters in length and are not case-sensitive (a is the same as A). As you type, Norton AntiVirus replaces the characters on the screen with asterisks (*) for security.

6 Click OK in the Set Password dialog box.

7 Click OK.

Norton AntiVirus will also prompt for the password before allowing changes to the password protection options.

To change your password:

1 Click Options in the Norton AntiVirus main window.

2 Click the Password tab (see Figure 5-16).

3 Enter your existing password in the Verify Password dialog box that appears.

4 Click Set Password.

5 Enter your existing password in the Old Password text box.

6 Enter the new password in the New Password text box; then type it again in the Confirm New Password text box.

7 Click OK.

To remove password protection:

1 Click Options in the Norton AntiVirus main window.

2 Click the Password tab (see Figure 5-16).

3 Enter your existing password in the Verify Password dialog box that appears.

4 Do one of the following:

   - To remove password protection completely, uncheck Password Protect.
   - To remove password protection for some of the protected features, select Custom Password Protection and click items in the list box to deselect them.

5 Click OK.

About computer viruses A

Protecting computers with properly configured antivirus software has become a requirement for everyday safe and secure computing. Although estimates of the actual number of detectable computer viruses vary dramatically, roughly 8000 are believed to be in existence. This number reflects the fact that many identified viruses have multiple strains. A virus author can effectively create a new virus strain by changing as little as a single byte in an existing virus's code.

Virus authors often communicate through BBSs and Internet sites where they can chat about their activities and exchange tools and code. The majority of viruses, however, are not distributed beyond the boundaries of this virus-writing subculture. Only a fraction of the viruses in existence are released "in the wild"; that is, released in environments likely to be accessed by the general computing public.

In general, the level of talent of the average virus author is unimpressive, even when compared to the abilities of entry-level professional programmers. Many viruses are not written to deliberately interfere with a computer's operation, yet because the author has made so many errors in writing the virus, programs and data are subject to reckless destruction.

Whatever their source, the number of known viruses and infection incidents continues to increase:

- Many destructive viruses have already made their way into the wild.
- An ever-increasing number of virus types and strains continues to threaten the general computing population.
- The potential costs related to viral damage are astronomically high.

What are computer viruses

Computer viruses are, simply, executable computer programs. Like biological viruses, they find and attach themselves to a host. Just as a cold virus finds and attaches itself to a human host, a computer virus attaches itself to an item, such as a computer start-up area (boot record) or an executable file.

After a computer virus attaches to, or infects, a file or other part of your system, it spreads to neighboring items. Attaching itself to an item that is widely used by the general public or where file sharing is common, allows the virus to spread as widely as possible. The more successful the virus is in spreading, the greater its chances of survival.

There are many common misconceptions about what computer viruses actually do and what they are incapable of doing. For example,

A virus can infect...

- Program files, non-file areas used on computer start-up (boot records), and data files with macro capabilities
- Data disks and disks used to transfer programs
- Your computer when you download and use files from an online service
- A file before it is attached to an e-mail message

A virus cannot infect...

- Hardware, such as keyboards and monitors, graphic files, data files without macro capabilities, software items other than program files
- Write-protected disks
- Your computer when you read messages from an online service
- Text-based e-mail messages

Trojan horse programs are often confused with computer viruses. Because they don’t replicate and spread, they are not viruses.

A Trojan horse is a program that appears to serve some useful purpose or to provide entertainment. This guise encourages you to run it. But, like the Trojan horse of old, it also serves a covert purpose which may be to damage files or plant a virus on your computer.

Infection

Computer viruses are activated when you execute (or run) an infected program or start up a computer with infected boot records. Once activated, computer viruses spread in one of two ways depending on their design:

- Direct Action Infector
- Memory Resident Infector

A Direct Action Infector virus is activated when an infected file is executed. It takes control of the system before other software can load and looks for “clean” files to infect. When the infected program is closed, the virus stops infecting.

A Memory Resident Infector virus is much like a conventional terminate-and-stay-resident program (TSR). It hooks (takes over) the system when activated. A memory resident infector maintains control of the system and continues to spread as you use your computer until memory is cleared (by rebooting), even if you close the infected program.

Trigger

Some, but not all, authors program their viruses to include an arbitrary incubation period. Once such a virus has made its way onto the computer, it waits to be activated by a trigger. Some of the many events that can act as triggers are a specific date, the count of sixty minutes after an infected program is executed, or the seventh program file that the virus program encounters. Other viruses use a random trigger.

Payload

Like a firearm, when the trigger is activated, an activity known as a payload occurs. Note that some viruses do not wait for a trigger, but deliver their payload whenever they are activated.

Some payloads are willfully destructive, such as those that format hard drives or corrupt files, while others are benign, doing little more than displaying a message on a computer screen. For example, a file infected with the Windows 95 Boza virus displays a lengthy message that begins with, “The taste of fame just got tastier!” (the payload) on the 30th day of any month (the trigger).

Viruses don’t necessarily let you know that they’re there, even after they do something destructive. For example, the Ripper virus will make random changes to files on a disk so slowly that the changes go unnoticed by the average computer user.

Virus targets

Viruses are categorized by their infection targets:

- Program viruses infect program files, which commonly have extensions such as .COM, .EXE, .SYS, .DLL, .OVL, or .SCR. The most common programs targeted by viruses are standard DOS programs which use the .COM and .EXE file extensions. Program files are attractive targets for virus writers because they are widely used and have relatively simple formats to which viruses can attach.

- Boot viruses infect the non-file (system) areas of hard and floppy disks. These areas offer an efficient way for a virus to spread from one computer to another. Boot viruses have achieved a higher degree of success than program viruses in infecting their targets and spreading.
- Macro viruses infect data files with macro capabilities and are the newest threat to the computing public. For example, Microsoft Word document and template files are susceptible to macro virus attacks. They spread very rapidly as infected documents are shared on networks or downloaded from Internet sites.

Each virus type, which uses a different mechanism to infect its particular target, is discussed in the following sections.

Program viruses

Like normal programs, program viruses must be written for a specific operating system. The vast majority of viruses are written for DOS but some have been written for Windows 3.x, Windows 95, and even UNIX.

All versions of Windows are compatible with DOS and can host DOS viruses with varying degrees of success. The following table describes how DOS program viruses behave in the different versions of Windows.

Windows version	Description of virus behavior
Windows 3.x	Most DOS viruses thrive in this environment because Windows 3.x uses DOS for all of its basic file functions.
Windows 95	Windows 95 is designed to be fully compatible with almost any older program, including program viruses. When a memory resident infector that attacks boot records is active, Windows 95 may display warnings during startup and your system’s performance may degrade.
Windows NT	Windows NT provides the least degree of DOS compatibility, but it still hosts program viruses quite well. On Windows NT, memory resident infectors only infect and spread in a DOS session. If you close the DOS session, the virus is deactivated until you run an infected program in another DOS session. Also, because NT provides file security, program viruses can’t infect or damage files you can’t access.

Boot viruses

All hard and floppy disks have boot records, whether or not they also contain operating system files. A disk does not have to be bootable to be infected by a boot virus; data disks can contain boot viruses too. A typical way a computer gets a boot infection is to restart with an infected floppy disk inadvertently left in the drive. Even if the floppy is not a boot disk, the virus will activate and spread.

Unlike program viruses, almost any boot virus can infect DOS, Windows 3.x, Windows 95, Windows NT, and even Novell Netware systems. This is because they exploit inherent features of the computer (rather than the operating system) to spread and activate.

Many boot viruses assume the hard disk is using a normal DOS file system. Such an assumption is not always correct if you are using an operating system other than DOS or Windows 3.x. On Windows NT, for example, you can choose to use the NTFS file system instead of the DOS-compatible FAT file system. If a virus encounters a system using NTFS, it still successfully infects the computer but it may accidentally damage some of your files or boot records (disk system areas) in the process. When this happens, NT won’t be able to start and you may need to reinstall Windows.

Another interesting aspect of Windows NT is that it will disable any boot viruses when it starts, assuming it can still start. This means that boot viruses can infect a machine running Windows NT but they can’t spread to other systems while Windows NT is running. Don’t, however, assume that the virus is benign. Every time you boot your system, the virus activates and has a chance to activate its trigger and deliver its payload. For example, on March 6th, the Stoned.Michelangelo virus writes random bytes to every cylinder on the hard drive, corrupting the original data. In a fraction of a second, key non-file areas used on computer start-up are the first to be wiped out in the process. It is virtually impossible to prevent the virus from destroying all data on the hard disk once the destructive trigger routine has activated.

Macro viruses

Many older applications had simple macro systems that allowed you to record a sequence of operations within the application and associate them with a specific keystroke. Later, you could perform the same sequence of operations by merely hitting the specified key.

Newer applications provide much more complex macro systems. You can write entire macro-programs that run within the word processor or spreadsheet environment and are attached directly onto word processing and spreadsheet files. The ability to tote one or more macros around with a data file is a very powerful feature. Unfortunately, this ability also makes it possible to create macro viruses.

A typical chronology for macro virus infection begins when an infected document or spreadsheet is loaded; the application also loads any accompanying macros that are attached to the file. If one or more of the macros meet certain criteria, the application will also immediately execute these macros. Macro viruses rely upon this auto-execution capability to gain control of the application’s macro system.

Once the macro virus has been loaded and executed, it waits for you to edit a new document, then kicks into action again. It attaches its virus macro programs onto the new document, then allows the application to save the document normally. In this fashion, the virus spreads to another file and does so in a completely discrete fashion; you have no idea of the infection. If this new file is later opened on another computer, the virus will once again load, be launched by the application, and find other unsuspecting files to infect.

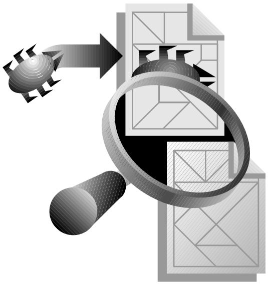
Finally, as far as a macro virus is concerned, the application serves as the operating system. A single macro virus can spread to any of the platforms on which the application is installed and running. For example, a single macro virus that uses Microsoft Word could conceivably spread to Windows 3.x, Windows 95, Window NT, and the Macintosh.

Virus technologies

Program and boot viruses are also categorized by the technology they use to replicate and attempt to avoid detection. Each is described in the following sections.

Stealth viruses

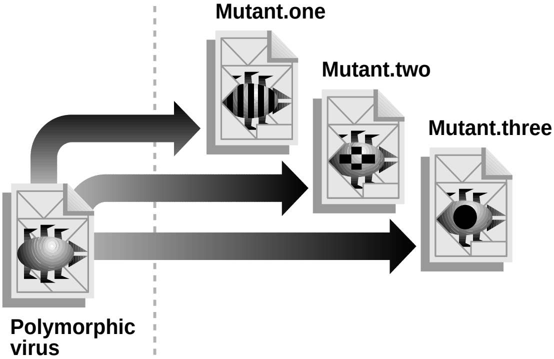
Stealth viruses actively seek to conceal themselves from attempts to detect or remove them. They use techniques such as intercepting disk reads to provide an uninfected copy of the original item in place of the infected copy (read-stealthing viruses), altering disk directory or folder data for infected program files (size-stealthing), or both.



For example, the Whale virus is a size-stealthing virus. It infects .EXE program files and alters the folder entries of infected files when other programs attempt to read them. The Whale virus adds 9216 bytes to an infected file; because changes in file size are an indication that a virus might be present, the virus then subtracts the same number of bytes (9216) from the file size given in the directory/folder entry to trick the user into believing that the file's size has not changed.

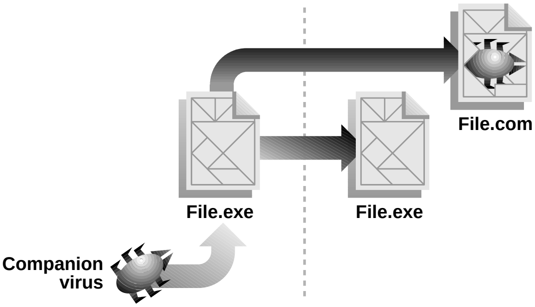
Polymorphic viruses

Most simple viruses attach identical copies of themselves to the files they infect. An antivirus program can detect the virus's code (or signature) because it is always the same and quickly ferret out the virus. To avoid such easy detection, polymorphic viruses operate somewhat differently. Unlike the simple virus, when a polymorphic virus infects a program, it scrambles its virus code in the program body. This scrambling means that no two infections look the same, making detection more difficult.



Companion viruses

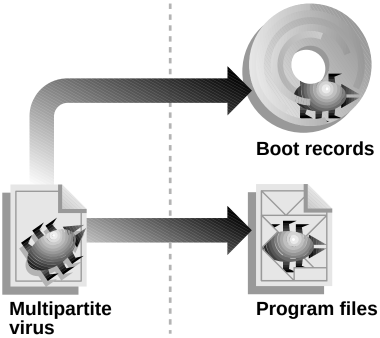
A companion virus is the exception to the rule that a virus must attach itself to a file. The companion virus instead creates a new file and relies on a behavior of DOS to execute it instead of the program file that is normally executed.



Companion viruses use a variety of strategies. Some companion viruses create a .COM file with a name identical to an existing .EXE file. For example, the companion virus might create a file named CHKDSK.COM and place it in the same directory as CHKDSK.EXE. Whenever DOS must choose between executing two files of the same name where one has an .EXE extension and the other a .COM extension, it executes the .COM file.

Multipartite viruses

Multipartite viruses are both program and boot viruses. For example, if you run a word processing program infected with the Tequila virus, the virus activates and infects your hard disk boot record. Then, the next time you boot your computer, the Tequila virus activates again and starts infecting every program you use, whether it is on a hard or floppy disk.



Keeping your protection current

Norton AntiVirus, using techniques that defeat any attempts viruses may make to avoid detection, detects viruses based on their telltale virus signatures. This information is stored in the Norton AntiVirus virus definitions files. Your protection against viruses is only as current as the virus definitions files your Norton AntiVirus product is using.

To maximize your computer's protection against new viruses, you must regularly update your virus definitions files. Symantec provides updated virus definitions files at no charge every month. You can get the new virus definitions files in a variety of ways, depending upon the product you are using. See Chapter 4, “Keeping up with new viruses,” on page 67 for detailed information and procedures.

The world of computer viruses is a dynamic one. Be sure to update your virus definitions files every month.

Using your Norton AntiVirus rescue disks

B

A Norton AntiVirus rescue disk set simplifies recovery from virus emergencies. The rescue set is composed of the following three disks:

- Norton AntiVirus Emergency Boot Disk: Used to start your computer.
- Norton AntiVirus Program Disk: Used to scan for and remove viruses.
- Norton AntiVirus Definitions Disk: Virus definitions files used during scans.

If you have not yet created a Norton AntiVirus rescue disk set, do it now. See "Creating a rescue disk set," on page 42.

Removing viruses from a shutdown computer

To remove viruses using your Norton AntiVirus rescue disk set:

1. If your computer is running, choose Shutdown from the Start menu on the Windows taskbar to shut down the computer.
2. Switch off your computer using the power switch. Turning off the power removes any viruses that might be present in memory.

   You must switch off the power. Selecting Restart or pressing Ctrl+Alt+Del is not sufficient to remove certain viruses from memory.
3. Place your disk labeled "Norton AntiVirus Emergency Boot Disk" in the A: drive, then switch on your computer. Your computer will start up from the rescue disk.
4. When prompted, remove your first rescue disk and insert the one labeled "Norton AntiVirus Program Disk."
5. Type `GO` at the DOS prompt, press Enter, then follow the on-screen directions.
6. Norton AntiVirus scans and informs you when the virus is found. Press R for Repair to eliminate the virus and repair the damaged item.

7 Once all viruses have been eliminated, remove any floppy disks and reboot your computer by switching the power switch off and then on to return to Windows.

8 Try to find the source of the virus. Start Norton AntiVirus and scan all hard drives again. Scan floppy disks as well.

If you don’t have a Norton AntiVirus rescue disk set, you can use the Emergency Disk that was supplied with your original Norton AntiVirus package. This disk, although not as powerful as a Norton AntiVirus rescue disk set, will detect and eliminate all common viruses.

To remove viruses without a Norton AntiVirus rescue disk set:

1 If your computer is running, choose Shutdown from the Start menu on the Windows taskbar to shut down the computer.

2 Switch off your computer using the power switch. This removes any viruses that might be present in memory.

You must switch off the power. Selecting Restart or pressing Ctrl+Alt+Del is not sufficient to remove certain viruses from memory.

3 Insert the Emergency Disk in the A: drive and switch on your computer. The disk must be in drive A: for your computer to start up from it.

4 Follow the on-screen instructions.

Restoring your hard disk

CAUTION: The following is an emergency procedure. Before you attempt to restore your hard disk, read the file called VIRSPEC.TXT located in your Norton AntiVirus folder or included with your virus definitions update. This file explains when you should or should not attempt this restoration.

There are a few situations when critical information about your hard disk is damaged by a virus and cannot be repaired. You can use your Norton AntiVirus rescue disk set to recover from these emergencies.

The error message that Norton AntiVirus returns, such as “Unable to repair boot record” or “Unable to repair master boot record,” determines how you use your rescue disks. Typically, you restore the CMOS data if your hard disk “disappears” or the number of drives or amount of memory is reported incorrectly.

master boot record partition table The first physical sector on a hard disk. It contains the master boot record program and the partition table, which stores information about how a hard disk is set up, such as the size and location of the partitions, which operating system each partition uses, and which partition the computer will boot from.

boot records The first logical sector of a hard disk partition. It identifies the disk’s architecture (sector size, cluster size, and so on). It also contains the boot record program.

CMOS An abbreviation for Complimentary Metal Oxide Semiconductor. A battery-powered chip in 80286 (and more advanced) computers that stores basic data about the system’s hardware.

If your rescue disk set is current, it is safe to restore all three items.

CAUTION: Never use Norton AntiVirus rescue disks that were created for another computer. Rescue disks are specific to the computer for which they were created. Always create new rescue disks for your computer if you install a new operating system and add or change hardware devices, such as hard disks, or increase memory (RAM). See “Creating a rescue disk set,” on page 42 for directions.

Because the Norton AntiVirus emergency programs run under DOS, not Windows, you have to navigate the dialog boxes using the keyboard. The mouse won’t work. Use the following keys to make your selections.

- Press the Tab key to cycle through all of the controls in a dialog box.
- Use the up arrow and down arrow keys to highlight a choice, such as a drive, in a group box.
- Press the Spacebar to check or uncheck a highlighted check box.
- Press Enter to activate the highlighted command button.
- To immediately activate any control or button, press and hold the Alt key, then press the highlighted letter of the control or button label. Release both keys.

To restore your hard disk:

1 Switch off your computer using the power switch.

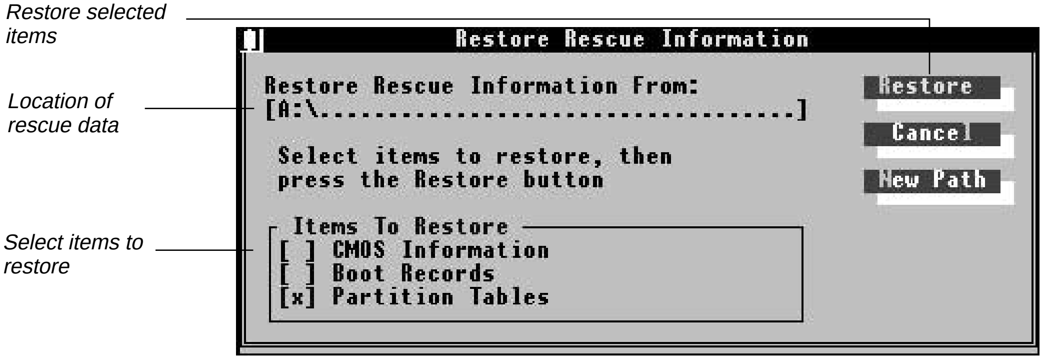
2 Place your write-protected Norton AntiVirus Emergency Boot Disk in the A: drive, then switch on your computer.

Your computer will start up from the rescue disk.

3 Type RESCUE at the A: prompt and press Enter.

The Restore Rescue Information dialog box appears.

Figure B-1 RESCUE main window



```
Restore Rescue Information

Restore Rescue Information From:
[A:\..................................]

 Select items to restore, then
 press the Restore button

 Items To Restore
[ ] CMOS Information
[ ] Boot Records
[x] Partition Tables
```

4 Make sure A:\ is specified for the location of the rescue data.

5 Check the items you want to restore in the Items To Restore group box. Items that are different from the stored information are checked automatically.

Press Tab to move around the dialog box. Press Spacebar to check or uncheck items.

6 Select Restore to restore the selected items.

7 When the process is complete, remove your Norton AntiVirus Emergency Boot Disk from the A: drive and restart your computer.

8 Start Norton AntiVirus and scan all hard drives again. Scan floppy disks as well to try to find the source of the virus.

Using command-line switches

C

A switch is an abbreviated command that you can use to direct a Norton AntiVirus activity or override default settings. The following Norton AntiVirus components can be run with command-line switches. When run without switches, these components all display a user interface instead.

- NAVDX.EXE performs startup scans and scans for viruses in emergency situations, such as after a virus alert shutdown.
- NAVW32.EXE is the Windows interface and scanner.
- RESCUE.EXE restores hard disk boot records, CMOS settings, and partition tables previously saved on your Norton Rescue Boot Disk. See “Creating a rescue disk set,” on page 42 for directions.

Some switches are used alone, while others are followed by a parameter, either a “+” or “-” sign. You can use more than one switch and more than one parameter on a command line. The pipe symbol (|) means that you should use either parameter, but not both. Do not type the brackets around the parameters on the command line.

NAVDX.EXE

DOS

NAVDX.EXE is the Norton AntiVirus component that performs startup scans and is run from the DOS prompt to scan for viruses in emergency situations, such as after a virus alert shutdown. See “Removing viruses from a shutdown computer,” on page 115 for more information.

Syntax

```
NAVDX [pathname] [options]
```

`pathname` Any drive, folder, file, or combination of these is scanned. If you want to scan a combination of items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files (for example, NAVDX A: C:\MYDIR\*.EXE).

`/A` All drives, except drives A: and B:, are scanned. Network drives are scanned if the Allow Network Scanning option is selected in the Scanner Advanced Settings dialog box.

`/L` All local drives, except drives A: and B:, are scanned.

`/S[+|-]` Enables (+) or disables (-) scanning of subfolders of any folders specified in the pathname.

`/M[+|-]` Enables (+) or disables (-) scanning of memory (for example, NAV C: /M+ or NAV D: /M-).

`/MEM` Only memory is scanned.

`/B[+|-]` Enables (+) or disables (-) scanning of boot records (for example, NAV A: /B+ or NAV B: /B-).

`/BOOT` Only the boot records of the specified drives are scanned.

`/PROMPT` Informs you when a virus is found and allows you to choose how to respond. The response choices available are determined by the items checked in the Buttons To Display If Prompted group box in the Options - Scanner Settings dialog box. See "Customizing manual scan options," on page 75 for more information.

`/REPAIR` Repairs an infected file without notifying you. The result is recorded in the Activity Log.

`/DELETE` Deletes an infected file without notifying you. The result is recorded in the Activity Log.

`/HALT` Shuts down your computer when a virus is found.

`/NOBEEP` NAVDX runs silently.

`/ZIPS` Scans files in compressed files

`/DOALLFILES` Scans all files, not just executables.

`/LOG:file` Creates a new log file.

`APPENDLOG:file` Adds to an existing log file.

`/CFG[:folder]` Specifies the folder containing program settings.

`/HELPERROR` Displays the DOS errorlevel codes that are returned.

`/?` Displays a brief description of all command-line switches available for NAVDX.

NAVDX also returns the following DOS errorlevel codes, which can be processed by batch files with the IF ERRORLEVEL statement. See your DOS documentation for more information.

Code	Error
0	No errors occurred and no viruses were found.
10	A virus was found in memory.
11	An internal program error occurred.
13	One or more viruses were found in the master boot record, boot sector, or files.
15	NAVDX self-check failed; it may be infected or damaged.
102	CTRL-C or CTRL-BREAK was pressed to interrupt the Scan.

Examples of usage

- To scan all .EXE files in your GAMES folder, type:

  ```
  NAVDX C:\GAMES\*.EXE
  ```

- To scan the GAMES folder on your hard disk, your D: drive, and the file C:\SAMPLES\SAMPLE.EXE, type the following at the DOS prompt:

  ```
  NAVDX C:\GAMES D: C:\SAMPLES\SAMPLE.EXE
  ```

  If C:\SAMPLES is the current folder, type:

  ```
  NAVDX C:\GAMES D: SAMPLE.EXE
  ```

- To scan a folder on the network drive P: called PROGRAMS and all of its subfolders, type:

  ```
  NAVDX P:\PROGRAMS /S+
  ```

  If you want to immediately repair any infected files found during this scan, type:

  ```
  NAVDX P:\PROGRAMS /S+ /REPAIR
  ```

- To scan memory only, type:

  ```
  NAVDX /MEM
  ```

- To scan only the boot records of drives C: and A: type:

  ```
  NAVDX C: A: /BOOT
  ```

NAVW32.EXE

NAVW32.EXE is the Windows interface and scanner. It can be run with command-line switches, typically from the Start menu RUN command, to override configuration settings. When scanning drives using command-line switches, Norton AntiVirus runs minimized, but will pop open on your screen if a virus is found.

Syntax

```
NAVW32 [[pathname] options]
```

`pathname` Any drive, folder, file, or combination of these is scanned. If you want to scan a combination of items, use a space to separate the items. You can use wildcards when specifying pathnames for a group of files (for example, NAVW32 A: C:\MYDIR\*.EXE).

`/A` All drives, except drives A: and B:, are scanned. Network drives are scanned if the Allow Network Scanning option is selected in the Scanner Advanced Settings dialog box.

`/L` All local drives, except drives A: and B:, are scanned.

`/S` All subfolders of any folders specified in the pathname are also scanned.

`/M[+|-]` Enables (+) or disables (-) scanning of memory (for example, NAVW32 C: /M+ or NAVW32 D: /M-).

`/MEM` Only memory is scanned.

`/B[+|-]` Enables (+) or disables (-) scanning of boot records (for example, NAVW32 A: /B+ or NAVW32 B: /B-).

`/BOOT` Only the boot records of the specified drives are scanned.

`/NORESULTS` No scan results are reported on screen.

Examples of usage

- To scan all .EXE files in your GAMES folder, type:

  ```
  NAVW32 C:\GAMES\*.EXE
  ```

- To scan the GAMES folder on your hard disk, your D: drive, and the file C:\SAMPLES\SAMPLE.EXE, use the RUN command and type the following:

  ```
  NAVW32 C:\GAMES D: C:\SAMPLES\SAMPLE.EXE
  ```

  If C:\SAMPLES is the current folder, type:

  ```
  NAVW32 C:\GAMES D: SAMPLE.EXE
  ```

- To scan a folder on the network drive P: called PROGRAMS and all of its subfolders, type:

  ```
  NAVW32 P:\PROGRAMS /S
  ```

- To scan memory only, type:

  ```
  NAVW32 /MEM
  ```

- To scan only the boot records of drives C: and A: type:

  ```
  NAVW32 C: A: /BOOT
  ```

- To specify paths with long filenames that contain spaces, use double quotes:

  ```
  NAVW32 "C:\Homework Helper"
  ```

RESCUE.EXE

RESCUE.EXE, run from the DOS prompt, restores hard disk boot records, CMOS settings, and partition tables previously saved on your Norton Rescue Boot Disk. See “Restoring your hard disk,” on page 116 for more information.

TIP: If you haven’t yet created a Norton AntiVirus rescue disk set, do it now. See “Creating a rescue disk set,” on page 42 for directions.

Syntax

```
RESCUE [/RESTORE[:location]] [/G0] [/BW|/LCD]
```

`/RESTORE`	Restore from a rescue disk.
`location`	Drive and directory of rescue files.
`/G0`	Disables graphical mouse and all graphical characters.
`/BW`	Improves display on black and white monitors.
`/LCD`	Improves display on LCD monitors.
`/?`	Displays a brief description of all command-line switches available for RESCUE.

Example of usage

- To restore rescue information from the A: drive:

  ```
  RESCUE /RESTORE:A:\
  ```

System messages

D

This appendix contains an alphabetical list of the error messages you may see while using Norton AntiVirus. Whenever an item such as <FILENAME>, <DRIVE>, or <VIRUS NAME> appears, it is replaced by an actual filename, drive, or virus name in the message on your screen.

Messages and their meanings

<FILENAME> has changed since inoculation.

The file has changed since it was inoculated. This does not necessarily mean the file is infected with a virus. You need to determine whether the change is legitimate or not. See "Responding to Auto-Protect inoculation alerts," on page 60 for more information.

Boot record has changed since inoculation.

Inoculation changes in a boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate. See "Responding to Auto-Protect inoculation alerts," on page 60 for more information.

The configuration file NAVOPTS.DAT not found.

Norton AntiVirus could not find the file that contains the configuration settings. Norton AntiVirus loaded with the default settings.

Error on drive <DRIVE>. Drive or device not ready.

Norton AntiVirus could not access the specified drive because the drive door is open or there is a problem with the drive.

The <VIRUS NAME> boot virus was found on drive <DRIVE>.

A virus was found in the boot record on the specified drive. To remove the virus, select the Repair command button. For more information, see "Responding to Auto-Protect virus found alerts," on page 57.

The <VIRUS NAME> virus was found in memory.

A virus was found in your computer's memory, which means it is active and possibly spreading to other files. See "Responding to Auto-Protect virus in memory alerts," on page 56 for more information.

The boot record of drive <DRIVE> has changed since inoculation.

Inoculation changes in a boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate. See "Responding to Auto-Protect inoculation alerts," on page 60 for more information.

The boot record of drive <DRIVE> is infected with the <VIRUS NAME> virus.

A virus was found in the boot record on the specified drive. To remove the virus, select the Repair command button. For more information, see "Responding to Auto-Protect virus found alerts," on page 57.

The boot record on drive <DRIVE> is infected with the <VIRUS NAME> virus. Unable to inoculate boot records and system files.

A virus was found in the boot record on the specified drive. Scan the drive to find and remove the virus, then inoculate the boot records and system files. See "Scanning for viruses," on page 31 for more information.

The boot records and system files of drive <DRIVE> are not inoculated.

Norton AntiVirus is configured to check for inoculation in the boot records and system files on your startup drive, and they are not inoculated. See "Inoculating files," on page 36 for more information.

The boot records and system files of drive <DRIVE> have changed since inoculation.

Inoculation changes in boot records and system files are likely to indicate the presence of an unknown virus. See "Responding to Auto-Protect inoculation alerts," on page 60 for more information.

The file <FILENAME> has changed since inoculation.

The specified file has changed since it was inoculated. This does not necessarily mean the file is infected with a virus. You need to determine whether the change is legitimate or not. See "Responding to Auto-Protect inoculation alerts," on page 60 for more information.

The file <FILENAME> in the compressed file <FILENAME> is infected with the <VIRUS NAME> virus.

A virus was found in a file contained within the compressed file. Uncompress the file, then scan the files to find and remove the virus. See "Responding to Auto-Protect virus found alerts," on page 57 for more information.

The file <FILENAME> is attempting to change the read-only attribute of file <FILENAME>.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See "Responding to Auto-Protect virus-like activity alerts," on page 58 for more information.

The file <FILENAME> is attempting to format the hard disk.

Norton AntiVirus is configured to notifying you because this is an activity that viruses sometimes perform. See "Responding to Auto-Protect virus-like activity alerts," on page 58 for more information.

The file <FILENAME> is attempting to write to <FILENAME>.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See "Responding to Auto-Protect virus-like activity alerts," on page 58 for more information.

The file <FILENAME> is attempting to write to the boot record of drive <DRIVE>.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See "Responding to Auto-Protect virus-like activity alerts," on page 58 for more information.

The file <FILENAME> is attempting to write to the master boot record of the hard disk.

Norton AntiVirus is configured to notify you of this operation because it is an action that viruses sometimes perform. See "Responding to Auto-Protect virus-like activity alerts," on page 58.

The file <FILENAME> is infected with the <VIRUS NAME> virus.

A virus was found in the specified file. To remove the virus you can delete the file or repair the file. See “Responding to Auto-Protect virus found alerts,” on page 57 for more information.

The file <FILENAME> is infected with the <VIRUS NAME> virus. The file was not inoculated.

A virus was found in the file Norton AntiVirus tried to inoculate. Scan the file and remove the virus, then inoculate the file. See “Inoculating files,” on page 36 for more information.

The file <FILENAME> is not inoculated.

Norton AntiVirus is configured to check files for inoculation. This file has not yet been inoculated. See “Responding to Auto-Protect inoculation alerts,” on page 60 for more information.

The file <FILENAME> may contain an unknown virus.

Norton AntiVirus has detected a change in the file that may indicate the presence of an unknown virus. To remove the unknown virus, you can repair the file or delete the file. Use caution when replacing the file; the replacement may contain an unknown virus too. See “Responding to Auto-Protect virus found alerts,” on page 57 for more information.

The file <FILENAME> was not allowed to change the read-only attribute of the file <FILENAME>.

Norton AntiVirus is configured to not allow the read-only attribute changes to files because it is an action that viruses sometimes perform. See “Monitoring for virus-like activities,” on page 96 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See “Scanning for viruses,” on page 31 for more information.

The file <FILENAME> was not allowed to format the hard disk.

Norton AntiVirus did not allow the specified file to format your hard disk because it is an action that viruses sometimes perform. See “Monitoring for virus-like activities,” on page 96 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See “Scanning for viruses,” on page 31 for more information.

The file <FILENAME> was not allowed to write to the boot record of drive <DRIVE>.

Norton AntiVirus did not allow the specified file to write to the boot record of the specified disk because it is an action that viruses sometimes perform. See “Monitoring for virus-like activities,” on page 96 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See “Scanning for viruses,” on page 31 for more information.

The file <FILENAME> was not allowed to write to the file <FILENAME>.

Norton AntiVirus is configured to not allow changes to program files because it is an action that viruses sometimes perform. See “Monitoring for virus-like activities,” on page 96 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See “Eliminating viruses detected during scans,” on page 49 for more information.

The file <FILENAME> was not allowed to write to the master boot record of drive <DRIVE>.

Norton AntiVirus is configured to not allow changes to the master boot record because it is an action that viruses sometimes perform. See “Monitoring for virus-like activities,” on page 96 for more information.

If you suspect a virus, scan your disks to find and eliminate the virus. See “Eliminating viruses detected during scans,” on page 49 for more information.

The master boot record of drive <DRIVE> has changed since inoculation.

Inoculation changes in the master boot record are likely to indicate the presence of an unknown virus. However, there are a few situations where this kind of change is legitimate. See “Responding to Auto-Protect inoculation alerts,” on page 60 for more information.

The master boot record of drive <DRIVE> is infected with the <VIRUS NAME> virus.

A virus was found in the master boot record on the specified drive. To remove the virus, select the Repair command button. For more information, see “Responding to Auto-Protect virus found alerts,” on page 57.

The master boot record on drive <DRIVE> is infected with the <VIRUS NAME> virus. Unable to inoculate boot records and system files.

A virus was found in the master boot record on the specified drive. Scan the drive to find and remove the virus, then inoculate the boot records and system files. See "Eliminating viruses detected during scans," on page 49 for more information.

Not enough memory for desired operation.

Your computer does not have enough conventional memory to load Norton AntiVirus because there are terminate-and-stay-resident programs taking up space in conventional memory.

The system file <FILENAME> is infected with the <VIRUS NAME> virus. Unable to inoculate boot records and system files.

A virus was found in the specified system file. Scan the drive to find and remove the virus, then inoculate the boot records and system files. See "Eliminating viruses detected during scans," on page 49 for more information.

Unable to access drive: <DRIVE>.

Norton AntiVirus could not access the specified drive because the drive door is open or there is a problem with the drive.

Unable to complete scan.

Norton AntiVirus found more problems (infected files or inoculation changes) than it can report at one time. Correct the problems reported, then scan again. Norton AntiVirus will report any additional problems it finds. See "Eliminating viruses detected during scans," on page 49 for information on resolving the problems found.

Unable to delete write-protected file <FILENAME>.

The file Norton AntiVirus is trying to delete is on a write-protected disk or in a folder for which you don't have write access.

Unable to find the virus definitions files.

The files that Norton AntiVirus uses to detect known viruses cannot be found. You should reinstall Norton AntiVirus or get updated copies of the virus definitions files. See the "Automatically updating virus definitions," on page 67 for information on getting updated virus definitions files.

Unable to inoculate boot records and system files on drive <DRIVE>.

Norton AntiVirus cannot inoculate the boot records and system files because of a disk error. Your disk may have cross-linked files or a hardware problem.

Unable to inoculate the file <FILENAME>.

Norton AntiVirus cannot inoculate the file because:

- You don't have read-write access to the inoculation file or folder.
- The file that Norton AntiVirus is trying to inoculate cannot be found. If you are inoculating a file on a network drive, the file may have been deleted between the time you selected the file to inoculate and the time that Norton AntiVirus attempted the inoculation.
- The file you are trying to inoculate is fewer than 32 bytes.

Unable to inoculate the specified folder.

The folder specified could not be found or you do not have read-write access to the inoculation file or folder. If you are inoculating a file on a network drive, the folder may have been deleted between the time you selected the folder to inoculate and the time that Norton AntiVirus attempted the inoculation.

Unable to open system messages file.

The system messages files are not in the Norton AntiVirus folder. Reinstall Norton AntiVirus.

Unable to print the requested information.

The data cannot be printed because the printer is not connected or not online.

Unable to read the boot record.

Norton AntiVirus was not able to access the boot record to check it for inoculation. This message can occur if you are using a program that locks the boot record in some way, preventing Norton AntiVirus from accessing it.

Unable to read the master boot record.

Norton AntiVirus was not able to access the master boot record to check it for inoculation. This message probably indicates a hardware problem. This message also occurs if you are using a program that locks the boot record in some way, preventing Norton AntiVirus from accessing it.

Unable to reinoculate boot records and system files on drive <DRIVE>.

The boot records and system files cannot be reinoculated because you don’t have read-write access to the inoculation file. See “Customizing inoculation,” on page 100 for information on the location of the inoculation file.

Unable to repair <FILENAME>. The file is still infected with the <VIRUS NAME> virus.

Norton AntiVirus was not able to remove the virus from the specified file. You can eliminate the virus by deleting the file. See “Responding to Auto-Protect virus found alerts,” on page 57 for more information.

Unable to repair boot record of drive <DRIVE>.

Norton AntiVirus was not able to repair a boot record on the specified drive. See “Restoring your hard disk,” on page 116 for more information.

Unable to repair master boot record of drive <DRIVE>.

Norton AntiVirus was not able to repair the master boot record on the specified drive. See “Restoring your hard disk,” on page 116 for more information.

Unable to repair system files.

The system files on your startup drive could not be repaired. To remove the virus, use the DOS SYS command from a write-protected bootable disk to restore the system files to an uninfected state. The SYS command is placed on your Norton Rescue Boot Disk.

Unable to repair the boot record of drive <DRIVE> with inoculation data.

Norton AntiVirus was not able to restore the boot record to its previous state. See “Restoring your hard disk,” on page 116 for more information.

Unable to repair the file <FILENAME> with inoculation data.

Norton AntiVirus was not able to restore the file to its previous state. You can eliminate a possible virus by deleting the file and replacing it with an uninfected backup copy. See “Responding to Auto-Protect inoculation alerts,” on page 60 for more information.

Unable to repair the file <FILENAME>.

Norton AntiVirus was not able to repair the file. It is still infected with an unknown virus. You can eliminate the unknown virus by deleting the file. See “Responding to Auto-Protect virus found alerts,” on page 57 for more information.

Unable to repair the master boot record with inoculation data.

Norton AntiVirus was not able to restore the master boot record to its previous state. See“Restoring your hard disk,” on page 116 for more information.

Unable to repair write-protected boot record of drive <DRIVE>.

The boot record you are trying to repair is on a write-protected floppy disk. Remove write-protection, then repair the boot record.

Unable to uninoculate the file <FILENAME>.

The file cannot be uninoculated because you don’t have read-write access to the inoculation file. See “Customizing inoculation,” on page 100 for information on the location of the inoculation file.

Unable to update activity log file.

The Activity Log could not be updated because you don’t have read-write access to it.

Unable to update exclude file.

The Exclusions List file could not be updated because you don’t have read-write access to it.

Unable to update inoculation file.

The inoculation file could not be updated because you don’t have read-write access to it.

Unable to update the inoculation file in write-protected folder.

You don’t have write access to the folder where the inoculation file resides.

Troubleshooting

E

This appendix explains how to resolve some common problems that may arise while you are using Norton AntiVirus. Follow the procedures provided here to try to solve these problems before calling Symantec Technical Support.

Solutions to common problems

My Norton AntiVirus Emergency Boot Disk doesn't work

Due to the number of product specific technologies used by manufacturers to configure and initialize hard disks, Norton AntiVirus cannot always create a bootable Norton Rescue Boot Disk automatically. If your Norton Rescue Boot Disk does not work properly, do one of the following:

- If you have a special boot disk for your computer, add it to your Norton AntiVirus rescue disk set. In a virus emergency, boot from that disk (first slide open the plastic tab on the back of the disk to make sure it is write-protected). Remove the disk and insert your rescue disk labelled "Norton AntiVirus Program Disk." At the DOS prompt, type `A:GO` and press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Norton Rescue Boot Disk bootable. Be sure to test your modified Norton Rescue Boot Disk.

Sometimes, your Norton Rescue Boot Disk does not work properly because you have more than one operating system installed, such as Windows NT and Windows 95. To modify the disk, do the following:

- Start up from your hard disk, insert your Norton Rescue Boot Disk in the A: drive, and, from a DOS prompt, type `SYS A:` and press Enter. This transfers the operating system to the rescue disk. Be sure to restest your Norton Rescue Boot Disk.

I've scanned and removed a virus, but it keeps infecting my files.

Cause: The source of the infection is a floppy disk.

Solution: Scan all floppy disks. See "Scanning for viruses," on page 31 for directions.

Cause: The virus may be contained in an executable file with a non-standard file extension.

Solution: Modify the Scanner options to scan All Files instead of Program Files. Scan all disks that you use and repair all infected files. Add any infected files' extensions to the program file extensions list.

See "Selecting which files to scan," on page 80 and "Specifying program file extensions," on page 81 for information on how to change the selection of files for scanning.

I receive repeated unknown virus found alerts for various applications.

Cause: You have copied a file that already contained an unknown virus onto a disk you use. The unknown virus is being detected when it infects a new program, but the original infected file is not being detected.

Solution: Modify the virus-like activity settings so that they are all set to prompt you when the virus-like activity occurs. In this way, you will receive a virus-like activity alert when the program containing the unknown virus attempts to write to a program file.

The name of the file containing the unknown virus is displayed in the alert. You must then delete the file. Use caution if you replace this file; the replacement may contain an unknown virus.

See "Protecting against unknown viruses with Virus Sensor," on page 94 for information on how Norton AntiVirus can detect unknown viruses.

Norton AntiVirus automatic protection fails to load when I start my computer.

Cause: Norton AntiVirus configuration settings are not correct.

Solution: See "Enabling and disabling Auto-Protect," on page 33 for directions to enable Auto-Protect. See also "Customizing startup protection," on page 98 to make sure memory and boot records are scanned at system startup.

Norton AntiVirus is not notifying me when I attempt to do things that I thought it would not allow, such as writing to a program file.

Cause: The virus-like activity settings are configured to allow this activity.

Solution: Norton AntiVirus does not check for the activity when the option is set to Allow. If you wish to be alerted of the activity, change the setting to Prompt.

See “Monitoring for virus-like activities,” on page 96 for more information.

Cause: The activity is excluded for the file.

Solution: Norton AntiVirus may not be alerting you to the attempt because it has been added to the Exclusions List. That is, you selected the Exclude button in a Norton AntiVirus virus-like activity alert or manually added it to the list. In this case, Norton AntiVirus no longer checks for the excluded file to perform the activity.

See “Managing exclusions,” on page 83 for more information.

Cause: The activity is not one that Norton AntiVirus monitors. The virus-like activities are described in “Monitoring for virus-like activities,” on page 96.

I’m getting alerts to inoculate files that I’ve already inoculated.

Cause: You may have moved or renamed the directory or file. Inoculation data includes the file’s pathname. Moving or renaming a file invalidates its inoculation data.

Solution: You must reinoculate the file. See “Inoculating files,” on page 36 for more information.

I receive inoculation change alerts for one or more data files.

Cause: The extension for the data files has been added to the program file extensions list, causing Norton AntiVirus to include them when inoculating. Data files change often and should not be inoculated.

Solution: Uninoculate all files with the extension (see “Uninoculating files or folders,” on page 39). Then delete the extension from the program file extensions list (see “Specifying program file extensions,” on page 81).

Solution: Exclude files for inoculation with the extension. See “Managing exclusions,” on page 83 for directions.

After repairing a program with Norton AntiVirus, it does not work properly.

Cause: Although Norton AntiVirus removes the virus, the virus may have damaged the file beyond complete repair.

Solution: You should replace the program with an uninfected original.

I am getting inoculation change reports on my program files since I installed a new version.

Cause: Installing a new version of a program replaces many of the files with new files that have the same names. These files have, therefore, legitimately changed since inoculation.

Solution: You should reinoculate the files. See "Inoculating files," on page 36 for more information.

Glossary

application

See program.

AUTOEXEC.BAT

Text file of commands that is executed automatically when your computer starts up. The commands set up the path and prompt, and start certain programs. *See also* CONFIG.SYS, startup folder.

(to) boot

To start the computer.

bootable disk

Disk that contains the operating system necessary to start, or boot, the computer.

boot record

First physical sector on a floppy disk or the first logical sector of a hard disk partition. It identifies the disk's architecture (sector size, cluster size, and so on). It also contains the boot record program.

boot record program

Program that is responsible for loading the operating system.

boot virus

Virus that infects the boot record program on both hard and floppy disks and/or the master boot record program on hard disks. A boot virus loads into memory before the operating system, taking control of your computer and infecting any floppy disks that you access.

bulletin board system (BBS)

On-line service that allows messaging, electronic mail, and file transfer between computer users via modem.

CMOS

Abbreviation for Complimentary Metal Oxide Semiconductor. A battery-powered chip in 80286 (and more advanced) computers that stores basic data about the system's hardware.

cold boot

Start your computer by switching on the power. A cold boot recycles your computer's random access memory, thus removing any viruses that might be present in memory. *See also* warm boot.

.COM file

See executable file.

command-line switch

Option that controls the operation of a program. Switches can be used when a program is executed from the operating system prompt or through the Run command in Windows.

compressed file
Single file or series of files that have been compressed into one file using a compression utility such as PKZIP or LHARC.

CONFIG.SYS
Text file containing commands that configure the system's hardware and that load device drivers. The file is automatically executed by the operating system when you start your computer.

data file
File that is created by or associated with an application and contains no executable code.

device driver
Memory resident program that is loaded from CONFIG.SYS or SYSTEM.INI at startup. *See also* terminate-and-stay-resident program.

directory
See folder.

download
Transfer a file from one computer system to another through a modem. Most frequently used when referring to the act of transferring a file from a bulletin board system.

dropper
Program that installs a virus on your computer. Droppers are not viruses, they are trojan horse programs. *See also* trojan horse.

exclusion
Condition or activity that you have instructed Norton AntiVirus to ignore in a particular file. For example, you may want Norton AntiVirus to ignore the DOS FORMAT program when it formats a floppy disk.

.EXE file
See executable file.

executable file
File containing a program that can be launched. Executable files generally have the following extensions: .COM, .EXE, .OVR, .OVL, .DRV, .BIN, or .SYS.

file server
Central disk storage device (or devices) connected to a network that provides network users access to shared applications and data files.

folder
Portion of a disk that you designate to store information about files. Folders make it easier for you to organize the files on your disk. Also called a directory.

infected file
File that contains a virus.

inoculate Generate information or data about a file that can be used to verify the integrity of the file at a later time.

inoculation file File containing inoculation data that is used during scans to verify file integrity. An inoculation file is created for each drive on which you inoculate files.

known virus Any virus that Norton AntiVirus can detect and identify by name.

launch Start or run an application.

.LHA file Series of files that have been compressed into one file using the LHARC utility.

load *See* launch.

macro virus Virus that infects document files. Generally, a macro virus is executed when an infected document is opened, saved, or closed, and spreads to other documents. Macros, which are small programs associated with document files, are used to automate tasks.

master boot record (MBR) First physical sector on a hard disk. It contains the master boot record program and information on how a hard disk is partitioned.

master boot record program Program that is responsible for directing the computer to load the boot record program from the bootable hard disk.

memory-resident program *See* terminate-and-stay-resident program.

multipartite virus Virus that infects and spreads from both program files and boot records.

operating system Master control program that is loaded into memory when you start up or boot your computer. It controls and manages all computer operations and programs.

partition table Table in the master boot record of a hard disk that specifies how the disk is set up, such as the size and location of the partitions, which operating system each partition uses, and which partition the computer will boot from.

pathname
Location of a file or folder on a disk. For example, if a file named QTR1.DOC is stored in the folder OFFICE on drive C:, the pathname for the file is C:\OFFICE\QTR1.DOC.

polymorphic virus
Type of virus that changes its telltale code segments so that it “looks” different from one infected file to another, thus making detection more difficult.

program
Executable file or group of files written for a specific purpose such as word processing or creating a spreadsheet.

program virus
Virus that infects executable program files, such as .COM, .EXE, .OVL, .DRV (driver), and .SYS (device driver) files.

RAM
See random access memory.

random access memory (RAM)
Computer’s working memory that determines the size and number of programs that can be run at the same time, as well as the amount of data that can be processed instantly.

read-only
Refers to a disk or file containing data that can be read, but cannot be written to or deleted.

reboot
To restart your computer. *See also* warm boot and cold boot.

registry
Database maintained by Windows 95 to store hardware and software configuration information.

reinoculate
To replace a previously inoculated file’s inoculation data with data for the file in its current state.

repair
To remove a virus from a file and return the file to its original, uninfected state.

scan
Systematic search for viruses that is performed by Norton AntiVirus.

shell
Program that provides the interface between the user and the operating system. In Windows 95, the shell maintains the desktop, or graphical user interface.

startup folder
Special folder in your Windows\Start Menu\Programs folder. Programs in this folder run automatically when Windows starts.

stealth virus
Virus that actively seeks to conceal itself from discovery or defends itself against attempts to analyze or remove it.

subdirectory
See subfolder.

subfolder
Folder within a folder.

system disk
See bootable disk.

system files
Files that make up the operating system.

taskbar
Desktop component that gives access to the Start menu and currently running programs. Auto-Protect and the Norton Scheduler place icons on the taskbar to remind you they are enabled.

terminate-and-stay-resident program (TSR)
Program that loads itself into random access memory (RAM) and remains there so that it can be instantly activated. The TSR is removed from memory when the computer is turned off.

trojan horse
Program that promises to be something useful or interesting (like a game), but covertly may damage or erase files on your computer while you are running it. Trojan horses are not viruses because they don't replicate and spread.

TSR
See terminate-and-stay-resident program.

uninoculate
To remove the inoculation data for a file, folder, or drive. *See also* inoculate.

unknown virus
Virus for which Norton AntiVirus does not contain a virus definition. *See also* virus definition.

virus
Self-replicating program written intentionally to alter the way your computer operates without your permission or knowledge.

virus definition
Virus information that allows Norton AntiVirus to recognize and alert you to the presence of a specific virus.

virus-like activity
Activity or action caused by other software that Norton AntiVirus perceives as the work of a possible unknown virus.

VxD
Virtual device driver. It is an operating system extension that manages a computer resource. Auto-Protect is an example of a VxD.

warm boot
To restart your computer by pressing Ctrl+Alt+Del or shutdown and restart. A warm boot can be detected and emulated by some viruses, so a virus in memory may still be there when the warm boot is complete. *See also* cold boot.

workstation

Computer that is attached to a network and is not the network server.

write-protected disk

Disk that cannot be written to. Write-protecting disks prevents viruses from infecting them. To write-protect a 5.25" disk, cover the notch on the side of the disk with an adhesive label (usually a tab included with boxes of disks). To write-protect a 3.5" disk, slide the lever on the back of the disk to uncover the hole through the disk.

.ZIP file

Series of files that have been compressed into one file (usually with a .ZIP file extension) using PKZIP.

Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software and services, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section “Worldwide Service and Support” at the end of this chapter.

Registering your Symantec product

To register your Symantec product, please complete the registration card included with your package and drop the card in the mail. You can also register via modem during the installation process (if your software offers this feature) or via fax to (800) 800-1438 or (541) 984-8020.

Virus definitions update disk

If you don’t have a modem to obtain virus definitions files using the Internet, Compuserve, America Online, or the Symantec BBS, you can order regular updates from Symantec to arrive by mail. This service requires a fee.

To order, do one of the following:

- In the United States, call (800) 441-7234.
- Outside the United States, contact your local Symantec office or representative.

Technical support

Symantec offers an array of technical support options designed for your individual needs to help you get the most out of your software investment.

World Wide Web

The Symantec World Wide Web site (http://service.symantec.com) is the doorway to a set of online technical support solutions where you will find the following services:

Interactive problem solver

Symantec’s online interactive problem solver (known as the Support Genie) helps you solve problems and answer questions about many Symantec products.

Product knowledgebases

Product knowledgebases enable you to search thousands of documents used by Symantec Support Technicians to answer customer questions.

FAQs

Frequently Asked Questions documents, also known as FAQs, list commonly asked questions and clear answers for specific products.

Discussion groups

Discussion groups provide a forum where you can ask questions and receive answers from Symantec online support technicians.

FTP

Point your Web browser to http://service.symantec.com to search for and download technical notes and software updates. You can also click the LiveUpdate button in programs enabled with this feature to automatically download and install software updates and virus definitions.

Other Symantec support options include the following:

America Online

Type Keyword: SYMANTEC to access the Symantec forum.

CompuServe

Type GO SYMANTEC to access the Symantec forum.

Symantec BBS

Set your modem to 8 data bits, 1 stop bit, no parity and dial (541) 484-6669.

Automated fax retrieval system

To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.

For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.

StandardCare Support

If you can’t access the Internet, take advantage of your 90 days of free telephone technical support (from the date of your first call) at no charge to all registered users of Symantec software.

Please see the back of this manual for the support telephone number for your product.

PriorityCare and PlatinumCare Support

Expanded telephone support services available to all registered customers. For complete information, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070, or visit www.symantec.com/techsupp/telesupp.html

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the previous version for 6 months after the release of the new version. Technical information may still be available through online support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will only be available for discontinued products through online services. See the section “Technical support” for online service options.

Customer Service

Symantec’s Customer Service department can assist you with non-technical questions. Call Customer Service to:

- Order an upgrade.
- Subscribe to the Symantec Support Solution of your choice.
- Fulfill your request for product literature or demonstration disks.
- Find out about dealers and consultants in your area.
- Replace missing or defective CDs, disks, manuals, etc.
- Update your product registration with address or name changes.

You can also visit Customer Service online at www.symantec.com/custserv for the latest Customer Service FAQs, to find out the status of your order or return, or to post a query to a Customer Service discussion group.

Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support Office for your region.

Service and Support offices

NORTH AMERICA

Symantec Corporation 175 W. Broadway Eugene, OR, 97401	(800) 441-7234 (USA & Canada) (541) 334-6054 (all other locations) Fax: (541) 984-8020
Automated Fax Retrieval	(800) 554-4403 (541) 984-2490

BRAZIL

Symantec Brazil Av. Juruce, 302 - cj 11 São Paulo - SP 04080 011 Brazil	+55 (11) 5561 0284 Fax: +55 (11) 5530 8869

EUROPE

Symantec Europe Ltd. Kanaalpark 145 2321 JV Leiden The Netherlands	+31 (71) 535 3111 Fax: +31 (71) 535 3150
Automated Fax Retrieval	+31 (71) 535 3255

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd. 408 Victoria Road Gladesville, NSW 2111 Australia	+61 (2) 9850 1000 Fax: +61 (2) 9850 1001
Automated Fax Retrieval	+61 (2) 9817 4550

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please call our Technical Support automated fax retrieval service, in the United States at +1 (541) 984-2490, choose Option 2, and request document 1400.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

Norton AntiVirus™ for Windows® 95

Disk Exchange and/or Replacement Form

DISK EXCHANGE: Norton AntiVirus for Windows 95 is available on 3.5" high-density disks. If you purchased a product that does not contain the correct disk size for your computer, you may exchange the disk. Fill out Section A and return 1) this form, 2) your original disk, 3) a shipping and handling payment of $4.95, to the address below.

DISK REPLACEMENT: After your 60-Day Limited Warranty, if your disk or CD-ROM becomes unusable, fill out Sections A & B and return 1) this form, 2) your damaged disk, 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement disks. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive disk replacements.

SECTION A - FOR DISK EXCHANGE *AND* REPLACEMENT

Please send me: ___ 3.5" high-density disk (exchange/replacement) ___ CD-ROM (replacement)

Name____

Company Name ____

Street Address (No P.O. Boxes, Please) ____

City ____State _______ Zip/Postal Code ______________

Country* ____________________________________ Daytime Phone ___________________________

Software Purchase Date____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

SECTION B - FOR DISK REPLACEMENT *ONLY*

Briefly describe the problem:____

____

Disk Replacement Price	$ 10.00
Sales Tax (See Table)	______
Shipping & Handling	$ 4.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), **CA** (7.25%), **CO** (3%), **CT** (6%), **DC** (5.75%), **FL** (6%), **GA** (4%), **IA** (5%), **IL** (6.25%), **IN** (5%), **KS** (4.9%), **LA** (4%), **MA** (5%), **MD** (5%), **ME** (6%), **MI** (6%), **MN** (6.5%), **MO** (4.225%), **NC** (6%), **NJ** (6%), **NY** (4%), **OH** (5%), **OK** (4.5%), **PA** (6%), **SC** (5%), **TN** (6%), **TX** (6.25%), **VA** (4.5%), **WA** (6.5%), **WI** (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (Check One):

___ Check (Payable to Symantec) Amount Enclosed $ _________ __ Visa __ Mastercard __ American Express

Credit Card Number ____ Expires _________

Name on Card (please print) _______________________________Signature _____________________

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR DISK EXCHANGE AND/OR DISK REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003
Please allow 2-3 weeks for delivery within the U.S.

SYMANTEC.™

Potential Virus Submission Procedure

If you suspect your system has been infected by an unknown virus, complete the requested information on this form. Then follow the procedure on the back of the form to create a “virus sample” floppy disk. Send the form and the floppy disk to Symantec at the address below. The engineers at the Symantec AntiVirus Research Laboratory will analyze your disk and inform you of the results. This is a free service provided to Norton AntiVirus customers as part of Symantec’s commitment to virus-free computing.

Symantec Corporation
AntiVirus Research Laboratory, Virus Definitions
2500 Broadway, Suite 200
Santa Monica, CA 90404

Do *not* write “Contains Live Virus” on the envelope or disk mailer (this upsets the post office). All disks become property of Symantec and will be destroyed.

Please provide the following information:

Working environments:

□ DOS (version __________) □ Windows 3.1 □ Windows 95

Potential virus is observed in which environments:

□ DOS (version __________) □ Windows 3.1 □ Windows 95

Have you loaded the most recent virus definitions?

□ Yes (date of VIRSCAN.DAT file _____________) □ No (date of VIRSCAN.DAT file _____________)

Has any other scanner identified a virus?

□ Yes (name and version of scanner ___________________________ virus reported_________________) □ No

Describe the observed virus behavior with as much detail as possible (include infected products, versions, and component information):

____

____

____

____

____

Your Name ____

Company Name ____

Street Address ____

City____________________________________ State ________ Zip/Postal Code ___________________

Country ______________________________Daytime Phone ____________________________________

Creating a Virus Sample Floppy Disk

If Norton AntiVirus reports that a file may be infected with an unknown virus or that inoculation data changed (for no legitimate reason), you may be infected with an unknown virus.

For inoculation changes:

- Did you install a new version of the application?
- Does the program modify its executable file with configuration information?
- Is it possible that the file was upgraded automatically on a network?

For unknown virus alerts:

- Have you updated your virus definitions file to the most recent version? See Chapter 4, "Keeping up with new viruses," on page 67 for directions to receive the most recent virus definitions file. Then scan again.

If you still think you have an unknown virus infection, use the following procedure to create a "virus sample" floppy disk. The engineers at the Symantec AntiVirus Research Laboratory will examine the disk and contact you with the results of their analysis. This is a free service provided to Norton AntiVirus users.

To create a virus sample floppy disk:

1. Start the potentially infected system from its own hard drive in MS-DOS SAFE mode.

   Press function key F8 before Windows 95 starts and choose "Safe mode command prompt only" from the on-screen menu.

2. Format a floppy disk with the potentially infected operating system.

   From the DOS prompt, type `FORMAT A: /S` and press Enter.

3. Copy the following files from the C:\WINDOWS\COMMAND folder to the floppy disk: MODE.COM, MEM.EXE, KEYB.COM, and XCOPY.EXE
4. Type `A:` and press Enter to change to the A: drive.
5. Type `PATH;` and press Enter (don't forget the semicolon) to remove the path from the environment temporarily.
6. Run the programs (ignore any screen messages). The engineers will be able to determine if they become infected.
   - Type `A:MODE` and press Enter.
   - Type `A:MEM` and press Enter.
   - Type `A:XCOPY` and press Enter.
   - Type `A:KEYB` and press Enter.
7. Copy any files whose inoculation data has changed without legitimate reason to the floppy disk in the A: drive.
8. Copy any other programs that you suspect are infected to the floppy disk in the A: drive.
9. Label the floppy disk with your name, address, telephone number, and the date of its creation. Write "Potential Virus" on the disk label.
10. Complete and send the form on the previous page with the floppy disk to Symantec. If there is not sufficient room to describe the observed behavior and symptoms on the form, use additional sheets. If appropriate, include printouts of screen captures.

    A Symantec engineer will contact you with the results of the disk examination.

Index